****

**Sample Information Security Program and Incident Response Plan**

**Disclaimer**

This sample document was developed to assist various industries and organizations. This document provides one example of how an organization can implement an information security program to identify and mitigate various threats to information and other organization assets. The areas included within this document are not intended to be all-inclusive of a comprehensive program, and there may be areas outside of this document that are relevant to your organization and should be addressed. This document as presented below should not be seen as the sole method to identify and address information security risks within your organization.

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 and supporting controls to protect customer information obtained in conjunction with providing financial services.

For institutions that fall under this guidance, this requires the identification of reasonably foreseeable risks, implementation of controls to reduce those risks, and regular assessment of the effectiveness of those controls. To fully address components of GLBA, areas such as vendor management and incident response are often incorporated into the program. Through oversight, monitoring, and regular updates, the program should effectively mitigate threats as those threats evolve.

For organizations that are not required to comply with GLBA, developing a similar program is a best practice recommended by various frameworks and industry experts.

**Instructions**

To use this document for your organization:

1. Delete the two cover sheets.
2. Review the policy thoroughly and:
	1. Edit or remove areas that are not applicable to your organization.
	2. Add details to reflect the current policies and procedures in place for your organization.
3. Complete a comprehensive risk assessment:
	1. Identify the sources of information that your organization must protect, known as covered information.
		1. Consider primary sources of this covered information.
		2. Consider ancillary systems that may ultimately grant access to covered information (e.g., remote access applications, backup software, password management tools).
		3. Consider applications that you do not host but in which you may be responsible for certain controls, such as user administration.
	2. Identify relevant risks and threats that could impact the confidentiality and security of this information.
	3. Quantify the potential likelihood, impact, and business risk for each data set.
	4. Document the existing controls that mitigate the identified threats. Consider controls relevant to the creation, maintenance, and destruction of covered data.
	5. Define the residual risk, which is the remaining risk after existing controls.
	6. Develop a plan of action to further mitigate any risks that are not mitigated to a level within your risk appetite.
4. Regarding incident response planning:
	1. Consult with legal counsel and/or your cyber insurance provider regarding your incident response and breach notification requirements and update this plan accordingly.
	2. Discuss procedures for incident containment and evidence preservation with your IT staff or support provider to ensure procedures are thoroughly documented and adequate for your institution.
5. Review your documentation periodically and update it to reflect relevant changes in threats, controls, policies, and procedures.

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

© 2024 Capin Technology LLC

**Information Security Program & Incident Response Plan**

**Revision History**

This section outlines changes to this policy per revision date.

|  |  |
| --- | --- |
| Revision Date | Revision Description |
| January 2015 | * Program was created and presented to the Board for the first time
 |
| March 2015 | * Technology and application risk assessments revised to focus on the impact of various vulnerabilities
* Added section for vulnerability management, including procedures for addressing zero-day vulnerabilities
 |
| September 2016 | * Enhancements to wording throughout
* Added information regarding third-party requests for information
* Updated Incident Response Plan per InTREx procedures
* Updated vendor management forms for initial and ongoing vendor due diligence per InTREx procedures for FDIC-regulated financial institutions
* Added residual risk column to risk assessments
 |
| March 2017 | * Technology and Application Risk Assessments renamed to be Threat and Asset Risk Assessments
* Enhancements to wording throughout and streamlined risk assessments
* Added Supplemental Risk Assessments section
 |
| May 2018 | * Annual update and enhancements to wording throughout
 |
| January 2020 | * Annual update and enhancements to wording throughout
* Moved technology and application risk assessments to appendices
* Removed separate Cybersecurity Program section and incorporated into the general Information Security Program documentation
* Added a Vendor Risk Assessment section and streamlined Vendor Management Oversight section
* Combined Third-Party Contractor section into Vendor Management section
* Enhanced procedures for requests for information
* Updated risk assessment to address new risk areas
 |
| May 2022 | * Annual update and enhancements to wording throughout
* Updated Notification section and Incident Summary Form of Incident Response Plan to address the new 36-hour reporting requirement for financial institutions that have experienced a qualifying cyber incident
 |
| January 2024 | * Annual update and enhancements to wording throughout
* Enhancements to support updated requirements within GLBA
* Acknowledgement of the FTC’s requirement for non-banking financial institutions to report security breaches
 |

**Table of Contents**

Introduction 6

Information Security Program 7

Purpose 7

Responsibility and Oversight 7

Risk Assessment and Mitigation 7

Control Implementation 9

Access Controls 9

Asset Management 10

Encryption 10

Application Development 10

Disposal and Retention of Data 10

Change Management 11

Activity Logging and Monitoring 12

Requests for Information, Maintenance, or Access 12

Control Testing and Monitoring 13

Employee Awareness 14

Vendor Management and Service Provider Oversight 15

Classification 15

New Vendors 16

Existing Vendors 16

Oversight 17

Maintenance 17

Incident Response Plan 18

Scope and Purpose 18

Contact Information 18

Incident Response Team 18

External Resources 19

Law Enforcement and Government Agencies 19

Third Parties 19

Issue Detection 20

Response Procedures 20

Triage (All Catalysts) 21

Catalyst: External Attacker 22

Catalyst: Constituent (non-employee) 23

Catalyst: Vendors 24

Catalyst: Organization 24

Notification (All Catalysts) 25

Closure (All Catalysts) 27

Appendix A – Risk Assessment Documentation 28

Threat Risk Assessment 28

Asset Risk Assessment 35

Appendix B – Vendor Relationship Management 41

Vendor Relationship Inventory 41

New Product / Vendor Evaluation Form 42

Annual Vendor Review Checklist 48

Confidentiality Agreement 50

APPENDIX C – Cybersecurity Threat Log 51

appendix D – Incident Response Documentation 52

Notice of Fraudulent Activity Letter 52

Informal 52

Formal 52

Sample Constituent Alert Letter 54

Incident Summary Form 57

# Introduction

The Organization is vulnerable to a multitude of internal and external risks and vulnerabilities. Due to the rising number of cybersecurity threats and reported industry breaches, the Organization has implemented this Information Security Program and Incident Response Plan to define the measures taken to address these cybersecurity threats and the possibility of vulnerability exploitation in the following three stages: protect, detect, and respond.

**Incident Response Plan**

**Information**

**Security
Program**

Cybersecurity is defined as protecting information security assets from attacks and unauthorized access. The Information Security Program addresses the cybersecurity controls and procedures that must be followed to protect the Organization’s assets and detect vulnerability exploitation. The Incident Response Plan dictates the procedures to be followed when a vulnerability has been exploited and an asset has been compromised or is at risk of being compromised.

The Organization defines confidential and/or sensitive information as any information meeting any of the criteria documented below. For purposes of this document, the term ‘constituent’ applies to <*insert applicable parties, including employees, contractors, customers, members, donors, students, faculty, patients, providers, or other applicable constituents*>.

* Information that is required to be maintained for the Organization’s continued success.
* Constituent information classified as Personally Identifiable Information (PII) or Protected Health Information (PHI).
* Cost, operating plan, constituent data, profits, markets (current and prospective), or similar information.
* *<Insert other details about what is deemed confidential or sensitive information>.*

# Information Security Program

## Purpose

The Information Security Program has been implemented to guide protection of the Organization’s assets and business operations. The purpose of the Program is to:

* Ensure the security and confidentiality of Organization and constituent information.
* Protect against threats and hazards to the security of information at rest and in transit.
* Protect against unauthorized access to or use of records that could result in substantial harm or inconvenience to any constituent.

## Responsibility and Oversight

The <*insert title, such as Information Security Officer*> has been designated as the Qualified Individual responsible for the oversight and implementation of the Program.

The <*insert applicable oversight body, such as Board of Directors or Board of Trustees*> is ultimately responsible for approval of the Program and oversight of the Qualified Individual.

To ensure the *<insert applicable oversight body>* remains updated on material matters related to the Information Security Program, the Qualified Individual will provide a written report at least annually on the overall status of the Program and the Organization’s compliance. At a minimum, the annual report will address the following areas:

* Overall status of the Information Security Program
* Risk assessment, risk management, and control decisions
* Service provider arrangements
* Results of testing
* Security events or violations and Management’s response
* Recommendations for changes in the Program

Where necessary, additional reporting will be provided prior to the annual report.

## Risk Assessment and Mitigation

This Information Security Program is based on a thorough risk assessment process. Management has performed an assessment of risks to the Organization’s information technology (IT) and information systems (IS) to identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, destruction, or other compromise of constituent or Organization information; estimate potential damage that could be caused; and determine the sufficiency of mitigating controls.

The risk assessment process is supported by two written assessments.

* The Threat Risk Assessment is a general risk assessment used to assess the risks presented by the technologies utilized by the Organization and to define the mitigation controls to limit and/or eliminate those risks. This Assessment evaluates threats, such as malware, hacking, social engineering, and software obsolescence, that could impact the Organization and its constituent data regardless of where that data is held.
* The Asset Risk Assessment is a more detailed risk assessment that identifies the risks associated with specific systems, applications, and other assets utilized. Systems can include applications that reside on the internal network and applications hosted externally. Appropriate controls, heavily consisting of authentication and application-specific controls, are implemented to mitigate these risks to an acceptable level.

These Risk Assessments are documented in the **Appendices** of this Program and are updated when new technologies, systems, or applications are implemented. In addition, new threats emerge daily, and existing controls must be monitored continuously for effectiveness and enhancements; therefore, a comprehensive review is also performed annually to ensure that the risks assigned are accurate and that all necessary controls have been implemented and documented.

The following terms are utilized in the Risk Assessment documentation.

* **Threat**: Potential for a person or thing to exercise a specific vulnerability, whether accidentally triggered or intentionally exploited.
* **Likelihood of occurrence**: Potential that the threat will occur.
* **Vulnerability**: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised, whether accidentally triggered or intentionally exploited, to result in a security breach or violation of the system’s security policy.
* **Potential impact**: Relative potential damage to the Organization if the threat occurs.
* **Risk rating**: The rating derived from the establishment of the likelihood and the impact of the threats defined.

|  |  |
| --- | --- |
| **Likelihood of Occurrence** | **Impact** |
| **High** | **Medium** | **Low** |
| **High** | High | High | Medium |
| **Medium** | High | Medium | Low |
| **Low** | Medium | Low | Low |

* **Data classification**: Designation of data based on secrecy, sensitivity, or confidentiality that determines the level of protection needed. The Organization will utilize the following three classifications.

	+ **Confidential:** Most sensitive data for internal use only. Unauthorized disclosure would be extremely detrimental. This data warrants the highest level of control.
	+ **Sensitive**: Data where unauthorized disclosure would have a negative impact.
	+ **Public**: Information that is publicly available or information where unauthorized disclosure of such data would not have a serious negative impact. Appropriate controls will be implemented where beneficial and cost efficient.
* **Controls in place**: Controls implemented to prevent the threat from occurring, minimize the probability of occurrence, or detect the occurrence.
* **Residual risk**: The risk level that is still present once controls have been implemented.

At the completion of the risk assessment process, Management will review the residual risks for each identified threat. Management will aim to always have a very low residual risk with sufficient controls to lower this risk to a level that Management is willing to accept. In the event that existing controls do not mitigate risks to an acceptable level, Management will develop a plan of action to address the risk. Such actions could include the following.

* Implementation of additional control layers to further reduce the risk
* Transfer of risk through purchase of insurance or another arrangement
* Formal acceptance of the risk after evaluation of mitigating factors

In addition to the Threat and Asset Risk Assessments, the Organization also maintains other risk assessment documentation to identify foreseeable threats. The following have been implemented to assess various products, services, technology, and vendor dependencies. These documents should be referenced for a complete understanding of the control framework.

*<Insert applicable document names and where they can be accessed. The areas below are likely applicable to financial institutions such as banks or credit unions.>*

* **ACH Risk Assessment**: identifies reasonably foreseeable threats to the ACH receiving and origination functions
* **Cybersecurity Assessment Tool**: utilizes the FFIEC’s Cybersecurity Assessment Tool to determine the inherent risk profile rating and maturity level to identify the steps needed to advance to the next maturity level
* **Authentication Risk Assessment**: addresses the FFIEC’s Authentication and Access to Financial Institution Services and Systems guidance and assesses the risks and mitigating controls related to digital banking services and financial institution information systems

## Control Implementation

Controls have been implemented to reduce the inherent risk associated with threats to the assets, technology, and operations identified in the risk assessment process. Management aims to reduce the risk to the lowest level possible that remains within the Organization’s risk appetite.

In addition to the controls documented within the Risk Assessments or other supporting policies, the following provides an overview of several critical control areas. This list of controls is not exhaustive and there may be other protections deployed throughout the Organization to mitigate risks. Supporting policies, risk assessments, and other documentation should be considered when evaluating the entirety of the control framework.

### Access Controls

The Organization has implemented technical and physical access controls to protect against the unauthorized acquisition of constituent and Organization information. Such controls ensure authorized users are authenticated and granted access to customer information. They also limit authorized users’ access to only the information they need to perform their job duties or functions.

* *<Insert necessary details supporting this policy statement>*

For information systems that provide or have the potential to provide access to constituent information, access controls will include multi-factor authentication (MFA) unless the Qualified Individual has approved, in writing, the use of reasonably equivalent or more secure access controls.

* *<Insert necessary details supporting this policy statement>*

### Asset Management

The Organization will identify and manage its assets, including the data, personnel, devices, systems, and facilities to ensure the assets remain protected and secure. The Organization has implemented a variety of control layers to support its assets, such as inventorying processes, firewalls and intrusion detection systems, anti-malware protections, patch management procedures, etc.

* *<Insert necessary details supporting this policy statement>*

### Encryption

All constituent information that is held or transmitted by the Organization will be properly encrypted in transit over external networks and at rest. In the event encryption of such information is infeasible, alternative compensating controls will be identified, implemented, documented, and approved by the Qualified Individual.

* *<Insert necessary details supporting this policy statement>*

### Application Development

In the event the Organization supports in-house development of applications for transmitting, accessing, or storing constituent information, procedures will be implemented to evaluate, assess, or test the security of such applications prior to deployment. For custom applications developed by third parties for use by the Organization, procedures will be established to consider the sufficiency of the development practices of the third parties.

* *<Insert necessary details supporting this policy statement>*

### Disposal and Retention of Data

The Organization recognizes the need to appropriately control information in both electronic and paper formats. At certain times, constituent and Organization information should no longer be retained as unnecessary retention of data increases the potential impact in the event of an incident or breach.

The Organization has developed a <insert policy name, such as Data Retention Policy> that defines the retention periods for various data sets. The retention periods consider requirements from GLBA and other laws and regulations, industry best practices, and operational needs. The <Data Retention Policy> is reviewed periodically to ensure it is sufficient to discourage the unnecessary retention of data.

In certain instances, a required or recommended data retention period may not be feasible because the information is necessary for business operations or other legitimate purposes, is otherwise required to be retained by another law or regulation, or targeted disposal is not reasonably feasible due to the manner in which the information is maintained. In these instances, a written exception will be documented and approved by the Qualified Individual.

When defined retention periods are met, data will be disposed of properly to ensure that constituent or confidential Organization data are rendered unrecoverable. Management understands that information may be present on internal computer system hard drives; hard drives or flash memory in photocopiers, scanners, and other document reproduction technology; and other electronic devices, and Management will ensure that information on these systems is removed or sanitized before disposal of equipment or return of the equipment to a lessor at the end of a lease period.

The following table summarizes the type of information or asset and the method of disposal.

* *<Insert necessary details supporting this policy statement>*

|  |  |
| --- | --- |
| **Type of Information** | **Method of Disposal** |
| **Paper documents** |  |
| **Backup media** |  |
| **Servers** |  |
| **Desktops, laptops, and thin clients** |  |
| **Mobile devices**(tablets and smart phones) |  |
| **Removable media** (USB drives, external hard drives, etc.) |  |
| **Document reproduction technology** *(e.g., scanners, copiers, multi-function printers)* |  |
| **Network devices** *(e.g., firewalls, routers, switches, etc.)* |  |
| **Internet of Things (IoT) devices** (e.g., smart TVs, thermostats, HVAC, etc.) |  |
| **ATMs** |  |

### Change Management

Change management processes have been implemented to ensure that changes to the Organization’s environment are implemented in a secure and controlled manner. Procedures will be implemented based on the risk associated with a change and may consider aspects such as management approval, documentation requirements, testing, backup requirements, rollback procedures, and processes for emergency changes.

* *<Insert necessary details supporting this policy statement>*

A component of change management includes managing the implementation of new technology. Management understands that the environment is not stagnant and that new technology, systems, and infrastructure will be implemented. Management has established procedures to aid in the evaluation of these new implementations to ensure that all risks are identified, mitigated, and monitored and included in existing risk assessment documentation. Initial risk assessments and due diligence will be conducted to evaluate the impact of the new implementation on the environment. Mitigating controls will be designed and implemented after approval from the appropriate level of Management. Applicable departments, relevant members of the affected user base, and members of information technology and security staff will be included in risk assessment processes. Sample risk assessment documentation that may be used to evaluate new implementations is included in Appendix A.

Change management processes will also consider the impact of significant software updates, upgrades, or security patches. Defined procedures will be established to ensure these changes are implemented in a secure and controlled manner and that such changes do not negatively impact security configurations previously established.

### Activity Logging and Monitoring

Critical user activities have been identified and controls have been implemented to log and monitor such activities to ensure the timely detection of any unauthorized use of, or tampering with, constituent or Organization data. When unauthorized activity is detected, it will be assessed and escalated in accordance with the Incident Response Plan.

* *<Insert necessary details supporting this policy statement>*

### Requests for Information, Maintenance, or Access

Requests for information about constituents and the Organization or access to facilities are periodically received, and Management is aware of the risk associated with fraudulent or unauthenticated requests. All requests should be properly authenticated regardless of the method of communication, and access to Organization locations and equipment will not be allowed on an unescorted basis. Management will include the discussion of these risks and required procedures in its annual employee training.

#### Requests Related to IT

If any request in relation to obtaining information about or access to IT equipment is received, regardless of the method of request, and you did not initiate the request, the IT Department should be contacted immediately to ensure that the request is handled appropriately.

#### Non-IT Requests

The following defines procedures for in-person, email, fax, and telephone communications with constituents and other third parties:

* **In-person requests**: A constituent or third party should provide a form of government-issued identification. The employee should confirm that the constituent is a valid requestor for the requested information. If a vendor is requesting access to specific employees, locations, data, or systems, confirmation should be obtained from the appropriate level of Management or the individual the third party is visiting. The visitor should always be escorted.
* **Phone call requests:** Employees receiving constituent requests via telephone will first require the constituent to disclose his <*insert applicable details to be verified, such as account number, constituent ID, name, student number, faculty number, employee ID, or Social Security number*.> Additional information should be requested to properly verify the identity of the caller, including <*insert details such as date of birth, additional signers on the account, when and where the account was opened, etc.*>. At least one piece of knowledge-based authentication information should be confirmed. Such information is not found in a constituent’s wallet and includes information such as <*date and amount of last deposit, a recent transaction, loan payment amount, secret code/PIN/password, etc.*>
* **Fax requests**: Constituents submitting information via fax should have his or her identity verified via call-back procedures and by comparing the signature on the fax to the signature on file. Call-back procedures should be performed utilizing the phone number on the constituent’s file. The request should not be processed until the constituent is reached via telephone and the identity is verified.
* **Email requests**: Since identity cannot be verified via unsecured email and email can be easily hacked or spoofed, any requests for information or maintenance about constituents, employees, or Organization systems should never be accepted or provided via unsecured email. Such requests include, but are not limited to, the following:
	+ Financial information about a constituent’s account, such as balance, notice if a check or payment has cleared, etc.
	+ Request for details related to the IT environment, such as IP addresses, login credentials, etc.
	+ Requests to update constituent or employee information, such as address, phone number, email, or payroll account information
	+ Password or PIN resets to various systems
	+ Request to grant remote access that you did not initiate

The Organization cannot always control what the constituent sends, and there may be instances where a constituent or third party submits confidential information or requests maintenance via an unsecured method. In these instances, it is important to educate the individual that such requests will not be accepted via email. Employees are discouraged from responding to these emails, and steps should be taken to contact the individual via the telephone number on file to alert him of the proper process to submit the request. If the individual cannot be reached by phone, the employee can respond via email to provide this information, ensuring that any sensitive information has been removed from the body of the reply.

Employees are not to utilize information that is submitted to the Organization through an unsecured method.

* **Text requests**: Requests via text message are not currently deemed an acceptable method of communication. The requestor should be contacted at the phone number on file, not by responding to the text message, of the proper way to submit the request.

Third parties requesting constituent information will be required to have the constituent’s approval for the Organization to provide the information. Constituent approval will require that the constituent be properly identified using the above identification procedures. Written authorization may also be required from the constituent before information is provided to the third party.

## Control Testing and Monitoring

The Organization acknowledges the importance of testing and monitoring the effectiveness of the key controls that have been established to safeguard constituent and Organization information and to identify attempted and actual attacks on or intrusions into information systems. Such testing may be performed by internal functions, external firms, or a combination and will incorporate a variety of mechanisms, including the following.

*<Insert necessary details supporting this policy statement.>*

* Key controls will be tested at least annually through scheduled internal reviews and/or external assessments.
* Social engineering simulations will be conducted throughout the year to determine if employees are abiding by confidentiality practices.
* Continuous monitoring will be implemented to support the real-time assessment and identification of threats on designated assets. Continuous monitoring efforts will be achieved through a variety of tools and technologies, including, but not limited to, *<describe type of solution, such as endpoint detection and response, extended detection and response, or other monitoring tools>.*
* Vulnerability scanning of external and internal assets will be conducted biannually. Additional assessments will be considered when there are material changes to operations or business arrangements or any other circumstances that could materially impact the information security program.
* Penetration testing will be conducted annually with a scope that is based on the results of the risk assessment.

Management will track the status of any assessment findings, vulnerability scan results, or penetration testing outcomes in a centralized system to ensure that all issues are resolved in a timely manner. Results will be summarized and presented to the <*insert applicable oversight body, such as IT Committee, Board of Directors, etc.*>.

In the event a deficiency cannot be addressed, the risk will be presented to the Qualified Individual and other Management, as necessary, for formal risk evaluation and acceptance.

## Employee Awareness

It is critical that every employee is familiar with this Program and with information security best practices, and Management understands the importance of providing personnel with the necessary support to ensure they remain updated on risks identified by the risk assessment.

Employees will sign the *<insert policy name, such as Acceptable Use Policy (AUP)>* *<insert frequency, such as upon hire and annually thereafter>* acknowledging that he or she understands the Organization’s policies and information security best practices. Any employee violating these guidelines will be subject to disciplinary action.

Training will also be held for all employees upon hire and annually thereafter and will include the following minimum areas.

* *<Insert applicable details about the training provided.>*
* Current threat and breach information (e.g., social engineering such as phishing, call center and email fraud, malware, account takeover, etc.)
* Data security to include electronic and physical document storage and destruction
* Email security and web browsing issues
* Incident reporting procedures, including how to identify and escalate an issue
* Social networking acceptable use
* Workstation, laptop, and mobile device acceptable use and security
* Requirements for protecting constituent information

Training content will be assessed at least annually to ensure it continues to address the threats identified in the risk assessment.

Management also understands the importance of utilizing qualified information security personnel to support the information security function and manage information security risks, and procedures have been established to ensure information security personnel remain knowledgeable on current threats and countermeasures. Some steps taken to support this awareness include, but are not limited to, the following.

*<Insert necessary details supporting this policy statement.>*

* A rigorous hiring process has been established to ensure appropriate personnel are hired to support the information security function.
* The *<insert position such as Information Security Officer>* monitors resources and alerts from relevant sources to ensure that new threats are incorporated into risk assessment documentation and mitigated to an acceptable level. Sources reviewed include, but are not limited to, the following: <*insert applicable sources*>.
* The information security department meets on a <*insert frequency, e.g.* *weekly*> basis to discuss ongoing issues and any evolving threats.
* The information security department staff attend designated webinars and conferences.
* The Information Security Officer participates in peer groups with the <*insert applicable agency or group*>.

Finally, the <*insert applicable oversight body, such as Board of Directors or Board of Trustees*> will also be made aware of current threats and information security practices on an ongoing basis. At a minimum, this is done through the annual status report on the Information Security Program.

## Vendor Management and Service Provider Oversight

The Organization outsources various applications, technology, and functions to technology service providers and utilizes services from these vendors. The Organization maintains a certain level of dependence on these vendors. The vendors may access or store varying amounts of constituent data or have remote access capabilities to the Organization’s data, network infrastructure, and systems. Therefore, proper due diligence should be performed when the vendors are initially contracted and periodically thereafter to ensure that the Organization can select and retain service providers capable of maintaining appropriate safeguards over its internal and constituent information.

### Classification

Vendors will be classified based on risk and according to the following criteria. These criteria will dictate the level of due diligence required prior to contracting and on an ongoing basis. Each classification will be reviewed annually for existing relationships and adjusted as necessary. See **Appendix B** for a listing of all vendor relationships and the current classifications.

*<Update these classifications to meet your internal needs>*

* **Critical**: These vendors have the highest level of risk to the organization. These vendors meet one or more of the following criteria and will undergo the highest level of review at least annually.
	+ Has regular access to sensitive constituent or organization data.
	+ Has regular direct and/or unattended access to the organization’s network.
	+ Provides a critical service to the organization that would be hard to replace and detrimental if the vendor went under.
	+ Is responsible for hosting critical data and maintains the responsibility for securing and backing up this data.
* **Significant**: These vendors are extremely important to the organization; however, the vendors do not meet the criteria of a critical vendor. These vendors will undergo a detailed review every <*three*> years.
* **Non-Critical**: These vendors present the lowest level of risk to the organization. These include a limited number of individuals who have access to Organization premises and systems. These individuals include outside consultants, accountants, examiners, auditors, janitorial staff, and maintenance workers. These vendors will undergo the lowest level of review. If the vendors have access or potential access to Organization systems or constituent data, or locations where these may be stored, review will include obtaining confidentiality agreements and reviewing procedures for notifying the organization of a potential issue, breach, or compromise of constituent or organization information. The sample Confidentiality Agreement can be found in **Appendix B**.

###

### New Vendors

Upon selecting a new vendor, a complete risk assessment will be performed utilizing the New Product/Vendor Evaluation form in **Appendix B**. Depending on the services provided by the vendor and the level of access that the vendor has to sensitive data or Organization systems and infrastructure, the following areas will be reviewed:

* Financial viability
* Operational information
* Confidentiality practices
* Information security controls and cybersecurity preparedness
* Vulnerability management
* Insurance, with emphasis on cybersecurity coverage
* Incident response and breach notification
* Business continuity and disaster preparedness
* Compliance reports
* Vendor management and subcontractor relationship

#### If a decision is made to move forward with a new relationship, the provider will be required by contract to implement and maintain necessary safeguards and protections as required by GLBA, NIST, or other industry standards, as applicable depending on the type of information stored, processed, or accessed. Depending on the level of risk and classification of the relationship, review of the contract by certain levels of Management and/or legal counsel may be required.

### Existing Vendors

Applicable vendors will also be reviewed annually to ensure ongoing oversight. Each year, Management will examine existing contracts and will request and review information from all key vendors that have access to confidential data and/or provide significant services. <*For financial institutions*> In addition to the areas above, the Organization will request regulatory examinations from the primary regulator. The Annual Vendor Review Checklist in **Appendix B** will be utilized to evaluate each vendor.

### Oversight

The <*insert applicable oversight committee or responsible individual, such as IT Committee, Vendor Management Committee, Information Security Officer, or Vendor Management Officer*> will be responsible for overseeing the vendor management process. Once all documentation has been requested, received, and analyzed, Management will make the decision to approve the new relationship or extend, modify, or discontinue the existing relationship. A summary of the documents reviewed and Management’s decision of the future of the relationship with the vendor presented annually to the <*insert applicable oversight committee such as IT Committee, Vendor Management Committee, Board of Directors, or Board of Trustees*> for final review and approval. The most recent approved vendor list can be found in **Appendix B**.

## Maintenance

This Program will be evaluated and adjusted periodically to ensure it remains sufficient to safeguard constituent and Organization information. The Program will be reviewed at least annually and in the event of the following scenarios.

* As a result of the completion of risk assessments
* As a result of any testing and monitoring procedures
* Upon material changes to operations or business arrangements
* Upon other circumstances that may have a material impact to the Program

# Incident Response Plan

## Scope and Purpose

The Information Security Program provides a summary of the various control procedures used to protect confidential information and reduce the risk of intrusion into Organization systems. These control procedures include multiple layers of controls, such as passwords, firewalls, network security settings, physical security, and many others. While the extensive control procedures are in place, the risk of intrusion can never be eliminated completely. Prevention and detection controls are critical; however, effective response procedures are also vital.

Management has developed the following Incident Response Plan to be used if there is unauthorized access to or use of confidential information. The purpose of this Plan is to allow the Organization to act quickly, minimize the damage, and learn from the incident. Most incidents are events relating to a computer or network; however, this Plan also includes procedures for human misuse of electronic information. This Plan also addresses breaches, which are realized incidents that include the loss of control, compromise, or unauthorized access or disclosure by an unauthorized person of constituent or Organization data.

## Contact Information

###

### Incident Response Team

An Incident Response Team has been established to handle incident response, and the Team consists of members of <*senior leadership, the IT Committee, and other representatives from numerous areas within the Organization*>. The primary members are responsible for fulfilling the responsibilities listed; however, if the primary contact cannot be reached, the alternate contact will be notified. Current members are listed below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position/Company** | **Responsibility** | **After Hours Contact Information** |
|  |  | Facilitator |  |
|  |  | Facilitator (Alternate) |  |
|  |  | IT |  |
|  |  | IT (Alternate)  |  |
|  |  | InfoSec |  |
|  |  | InfoSec (Alternate)  |  |
|  |  | Physical Security |  |
|  |  | Physical Security (Alternate) |  |
|  |  | Public Relations |  |
|  |  | Public Relations (Alternate) |  |
|  |  | Compliance |  |
|  |  | Compliance (Alternate) |  |
|  |  | Constituent Care |  |
|  |  | Constituent Care (Alternate) |  |
|  |  | Human Resources |  |
|  |  | Human Resources (Alternate) |  |

### External Resources

External resources may be necessary for providing mitigation strategies and will be relied upon on as needed once the Incident Response Team meets. External resources consist of individuals and companies with expertise in specialized areas as documented below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Primary Contact** | **Position/Company** | **Responsibility** | **Contact Information** |
|  |  | Legal |  |
|  |  | IT forensics  |  |
|  |  | Network/computer support |  |
|  |  | Insurance  |  |
|  |  | Constituent notification  |  |

### Law Enforcement and Governmental Agencies

After the initial detection, appropriate law enforcement branches, regulatory bodies, and government agencies will be notified. Legal counsel and/or compliance personnel will aid in determining requirements for notification.

|  |  |  |  |
| --- | --- | --- | --- |
| **Primary Contact** | **Position** | **Responsibility** | **Contact Information** |
|  |  | Police |  |
|  |  | Federal Reserve Bank |  |
|  |  | Federal Regulator |  |
|  |  | State Regulator |  |
|  |  | Federal Trade Commission |  |
|  |  | U.S. Secret ServiceElectronic Crimes Task Force |  |
|  |  | U.S. Secret Service Field Office |  |
|  |  | FBI Field Office |  |
|  |  | Internet Crime Complaint Center |  |
|  |  | Federal Student Aid Office (for higher education entities)  | [Breach Intake Form](https://fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity/cybersecurity-breach-intake) |

### Third Parties

Various third parties that the Organization conducts business with may need to be notified. Contracts have been reviewed to determine if the notification is required, and required notification is listed below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Primary Contact** | **Position/Company** | **Responsibility** | **Contact Information** |
|  |  | Business partners |  |
|  |  | Vendors |  |
|  |  | Card processors  |  |
|  |  | Media |  |
|  |  | Donors |  |
|  |  | Customers |  |

## Issue Detection

One of the most critical steps in incident response is detection and notification to appropriate parties. The Organization has implemented numerous automated and manual controls to assist in timely identification of potential issues. Such sources of identification can come from the following areas. Note that this list is not exhaustive of the actual controls and tools in place.

* Active Directory audit logs
* Anti-malware system
* Environmental monitoring systems
* File integrity monitoring software
* Firewall, IDS/IPS, and other network activity logs
* Help desk alerts
* Physical security systems
* Security information and event management (SIEM) systems
* System performance reports and logs
* *<This list should be edited to include actual details of manual and automated tools and controls utilized.>*

Where applicable, parameters have been configured in these systems to detect abnormal activity and provide alerts to appropriate personnel to trigger the incident response program.

It is also recognized that issue detection can often come from end-user employees and constituents. The communication path for these individuals has been communicated via employee and constituent ongoing training and awareness. Depending on the urgency of the concern, employees are encouraged to report incidents via phone or email to their immediate supervisor or a member of the IT Department, who will then notify a member of the Incident Response Team. Constituents are regularly provided with contact information for various personnel in the event they would like to report suspicious activities or concerns.

Information sharing is also key to combatting cybersecurity threats as an industry and the Organization will share threat information when doing so will not put the Organization at risk of disclosure of confidential information.

As necessary, Senior Management and the <*Board of Directors or Board of Trustees*> will be alerted to the identified attacks and will be kept abreast as corrective action is planned and implemented.

## Response Procedures

All incidents can be addressed in stages according to the initial catalysts. For the purposes of the Plan, four possible catalysts have been identified and incident procedures have been defined for each scenario. The four catalyst groups that can initiate an incident are as follows:

* External attacker
* Constituents (non-employee)
* Vendors
* Organization (employees)

The procedures for each group will begin with the first stage of Triage. The Triage stage consists of detection, identification, and notification of the incident. Once those steps are followed, subsequent procedures will be defined for each catalyst group. Subsequent procedures include Investigation (analysis, interpretation, reaction, and recovery), Containment (reducing impact and eradication), Analysis (tracking), and Final Recovery (lessons learned).

**Triage**

Detection

Identification

Notification

Investigation

Containment

Analysis

Recovery

Organization

Constituents
(non-employee)

Vendors

**Catalysts**

External Attacker

### Triage (All Catalysts)

1. Incident is brought to the attention of an employee through one of the methods noted above. Depending on the subject matter, the employee will notify his or her direct supervisor, the IT Department, and/or other applicable personnel.
2. The IT Department will document the issue (including all details they were provided). The IT Department will perform a quick analysis to determine if incident is a false positive.
	1. If a false positive, the event is logged as such and the incident is considered closed.
3. Employee will notify a member of the Incident Response Team (IRT), who will notify the Facilitator. The Facilitator will contact all members for an emergency meeting.
4. The following will be discussed and documented during the IRT emergency meeting.
	1. How was the incident detected?
	2. Is the incident still in progress?
	3. Can the incident be quickly contained?
	4. What data or property is threatened?
	5. What system or systems are targeted and where are they located physically and on the network?
	6. Does it appear that information has been accessed or misused?
	7. What is the severity of the current or potential impact to the Organization?
	8. How critical are those assets to the ongoing operations of the Organization?
	9. Will the response alert the attacker?
	10. What is the threat level category using the following criteria?

|  |  |
| --- | --- |
| **Category** | **Description** |
| 1 | A threat to public safety or life |
| 2 | A threat to sensitive data |
| 3 | A threat to computer systems |
| 4 | A disruption of services |

* 1. The threat level assigned will dictate the amount of time and resources assigned to the incident.
1. The IRT will then define the catalyst of the incident and will follow the procedures of one of the following catalyst groups: External Attacker, Constituent (non-employee), Vendor, or Organization.

### Catalyst: External Attacker

These procedures should be followed if an individual that is not acting as a constituent or vendor initiates the incident. Examples of incidents from the external attacker include the following:

|  |
| --- |
| **Possible Incidents** |
| * Active intrusion
 | * DNS records hack
 |
| * DoS/DDoS attack
 | * Website hack
 |
| * Property theft
 | * Vulnerability exploitation
 |
| * Worm/virus/spyware/botnet
 | * System or database hack
 |
| * Brute force attack against applications
 |  |

1. Investigate
	1. Interview the affected users.
	2. Analyze all information (interviews, logs, reports, etc.).
	3. Define plan to contain the incident and resolve the issue or provide alternative system.
2. Containment
	1. If system(s) hosted at the Organization, disconnect any affected systems and devices from the network to prevent further unauthorized access and to prevent the potentially compromised system from affecting other network resources. Do not turn off the system as this may compromise data within the system.
	2. If system(s) hosted at vendor, contact the vendor to discuss strategies for ceasing operation of the affected system/device.
	3. If feasible, change the firewall rules or enforce highly limited policies for incoming and outgoing traffic.
	4. Change any system password that could have been compromised or utilized during the incident.
	5. If email account was compromised, check for changes in email forwarding rules.
3. Analysis
	1. IT Department will review the affected systems that are isolated to determine if constituent or other sensitive data was accessed, leaked, deleted, or manipulated.
	2. External IT forensic firm should be utilized to determine the exact problem and ensure that system has been cleared of all issues.
	3. If the incident is vendor-related, the IT Department will work closely with the vendor and ensure the root of the problem has been identified.
4. Recovery (concurrent with other phases)
	1. If the incident has been resolved, the affected system(s) can be brought back online.
	2. If new systems must be implemented and restore processes conducted, the Business Continuity and Disaster Recovery procedures should be referenced for exact procedures.
		1. The original system will be held until the forensic holding period has been reached.
		2. The system will undergo appropriate procedures to ensure all issues have been eliminated.
	3. If the incident is vendor-related, then the vendor should be contacted to determine best recovery methods.
	4. If the incident directly affected constituents, notification procedures are documented in the “Notification” section.

### Catalyst: Constituent (non-employee)

These procedures should be followed if a non-employee constituent initiates the incident. Examples of such incidents include the following:

|  |
| --- |
| **Possible Incidents** |
| * Constituent’s computer or mobile device is hacked, or account information is stolen to initiate fraudulent wire transfers, ACH files, donations, etc.
 |
| * Constituent’s email hacked
 |
| * Constituent impersonated via phone, email, fax, text, etc.
 |
| * Other forms of account takeover
 |

1. Investigate
	1. Contact the constituent to verify fraudulent transactions or activity.
	2. Interview the affected constituents and employees about incident.
	3. Analyze all information (interviews, logs, reports, etc.).
	4. Follow the money trail and determine if any of the transactions can be stopped or reversed.
	5. Define a plan to contain the incident and resolve the issue.
	6. Remind the constituent to utilize the after-hours phone number *<insert number>* that was provided to them if any additional fraudulent transactions or activities are noticed.
2. Containment
	1. Reverse all suspected fraudulent transactions or activities.
	2. The affected constituent’s online account (e.g., Internet banking, donor management portal, etc.) should be closed and a new online account should be created.
		1. At a minimum, the password should be changed.
		2. Recommend the constituent operate from a different workstation.

*<The following procedure is applicable to financial institutions>*

* 1. Notify any other financial institutions or third parties involved in the transactions and discuss if transactions can be stopped and reversed.
		1. The directory for FED ACH routing number contact information can be accessed electronically at <https://www.frbservices.org/EPaymentsDirectory/search.html>
		2. A “fraudulent ACH file or wire alert” should be sent via Feedline or the equivalent.
		3. The Notice of Fraudulent Activity Letter in **Appendix D** can be utilized to notify the other financial institutions.
	2. A temporary hold should be placed on all transactions until out-of-band confirmations can be made.
1. Analysis
	1. The account manager, IT manager, and other applicable departments should discuss all factors and confirm root cause.
	2. External IT forensic firm should be utilized to determine the exact cause.
2. Recovery (concurrent with other phases)
	1. Consider closing the affected account(s) and opening new accounts.
	2. Determine how much money can be recovered using all available methods.
	3. Decide how much the Organization is legally required to return to constituent and then the amount the Organization is willing to return in addition to the required amount.
	4. Advise constituent to have computer and mobile device analyzed by an IT specialist to ensure that any malware has been removed.

### Catalyst: Vendors

These procedures should be followed if the incident pertains to a vendor. Such incidents include the following:

|  |
| --- |
| **Possible Incidents** |
| * Security breach
 | * Zero-day vulnerability
 |
| * Ransomware at vendor location
 |  |

1. Investigate
	1. Review the notification details the vendor provided.
	2. Determine if any of the internal systems are affected.
	3. Define a plan to contain the incident and resolve the issue.
2. Containment
	1. If internal systems are affected, immediately remove systems from the network.
	2. If necessary, disconnect the connection from the Organization to the vendor.
	3. If feasible, change the firewall rules or enforce highly limited policies for incoming and outgoing traffic.
	4. Monitor vendor’s incident response activities to ensure appropriate actions are taking place.
3. Analysis
	1. Review vendor’s actions and determine if the incident has been contained.
	2. Work with vendor to determine next recovery steps.
4. Recovery
	1. If incident has been resolved, the affected system(s) can be brought back online.
	2. If new systems must be implemented and restore processes conducted, the Business Continuity and Disaster Recovery procedures should be referenced.
		1. Hold original system until the forensic holding period has been reached.
		2. The system will undergo appropriate procedures to ensure all issues have been eliminated.
	3. The vendor should be contacted for further instructions.

### Catalyst: Organization

These procedures should be followed for incidents directly affecting the Organization or incidents initiated by an employee of the Organization. Examples of such incidents include the following:

|  |
| --- |
| **Possible Incidents** |
| * Employee leaks data
 | * Property theft
 |
| * System abuse
 | * System failure
 |
| * Employee clicks phishing link and installs malware, ransomware, etc. or provides login credentials
 | * Employee allows unauthorized access to the internal network
 |

1. Investigate
	1. Interview the affected users and employees.
	2. Analyze all information (interviews, logs, reports, etc.).
	3. Determine which employee(s) is the culprit.
	4. Define plan to contain the incident and resolve the issue or provide alternative system.
2. Containment
	1. If the employee(s) performed any action that is grounds for dismissal, escort the employee off the premises immediately.
	2. If system(s) is hosted at the Organization, disconnect any affected systems and devices from the network to prevent further unauthorized access and to prevent the potentially compromised system from affecting other network resources. Do not turn off the system as this may compromise data within the system.
	3. If system(s) is hosted at the vendor, contact the vendor to discuss strategies for ceasing operation of the affected system/device.
	4. If feasible, change the firewall rules or enforce highly limited policies for incoming and outgoing traffic.
	5. Change any system password that could have been compromised or utilized during the incident.
	6. Start the change password process for all systems and physical locks.
	7. If email account was compromised, check for changes in email forwarding rules or other configurations within the system.
3. Analysis
	1. The IT department will review the affected systems that are isolated to determine if sensitive data was accessed, leaked, deleted, or manipulated.
	2. External IT forensic firm should be utilized to determine the exact problem and ensure that system has been cleared of all issues.
	3. If the incident is vendor-related, the IT department will work closely with the vendor and ensure the root of the problem has been identified.
4. Recovery (concurrent with other phases)
	1. If incident has been resolved, the affected system(s) can be brought back online.
	2. If new systems must be implemented and restore processes conducted, the Business Continuity and Disaster Recovery procedures should be referenced for exact procedure.
		1. Hold original system until the forensic holding period has been reached.
		2. The system will undergo appropriate procedures to ensure all issues have been eliminated.
	3. If the incident is vendor-related, then the vendor should be contacted to determine best recovery methods.

### Notification (All Catalysts)

The Organization has several stakeholders with direct interest in an incident. Notification is at the discretion of the Incident Response Team (IRT); however, in some instances, notification is required based on the severity and context of the incident.

|  |  |
| --- | --- |
| **Stakeholders** | **Notification** |
| Employees | * Employees should be kept on a need-to-know basis during the incident. Employees risk relaying inaccurate information and risk discretion of notification.
* After the incident, the IRT will decide if and what the internal explanation will include.
 |
| Constituents (non-employee) | * Constituents will be directly notified if constituent information was disclosed during the incident, transactions involving constituent funds were involved, or if constituent credentials/accounts were compromised. Constituent information is defined in this as a constituent name, address, or phone number together with the SSN, account number, debit/credit card number, PIN, or password that would permit access to a constituent’s account.
* A Sample Constituent Alert Letter is included in **Appendix D**; however, this sample should be edited to reflect the current incident accurately. The marketing department and legal counsel should review this letter prior to mailing. At a minimum, notification to the constituent should include the following:
	+ Description of the incident
	+ Type of information accessed or misused
	+ Measures taken by the Organization to protect constituent information from further unauthorized access
	+ Telephone number for the constituent to call for information and assistance
	+ Reminder to constituent to remain vigilant over the next one to two years and to report suspected identity theft or further compromise to the Organization
* The IRT should determine if a letter or personal calls are more appropriate for maintaining the relationship with the constituent.
* The IRT will decide if the entire constituent base should be notified. Usually this is only necessary if it is known that the entire constituent base was compromised or if the incident is made public or was visible to many constituents. Notification can be made through several communication methods or a combination of methods, such as email, postal mail, or phone call.
 |
| Vendors | * Vendors, such as core processors or card processors, should be notified if the incident directly affects their systems due to the network connection between the Organization and the vendors. Vendor notification will not be necessary in most scenarios; however, the Organization’s vendors should be considered for notification after each incident.
 |
| Partners | The IRT will decide if any of the Organization’s business partners should be notified. Usually this is only necessary if the incident becomes public knowledge; however, in most instances, notification will not be necessary. |
| Public (Media) | * The IRT will decide if the incident was severe enough to warrant public notification. This is rare; however, in some instances is required to restore the Organization’s image.
 |
| Insurance | * The insurance provider should be notified, and a claim should be filed for any incidents involving electronic or physical theft/damage.
 |
| * Local Police
* FBI Field Office
* Internet Crime Complaint Center
* U.S. Secret Service
* Electronic Crimes Task Force
* U.S. Secret Service Field Office
* Federal Reserve
* Federal Regulator
* State Regulator
* Federal Student Aid Office
 | * Appropriate law enforcement and regulatory agencies should be notified at the discretion of the IRT.
* <*If a banking financial institution*> A Suspicious Activity Report (SAR) should be filed with the Financial Crimes Enforcement Network (FinCEN) utilizing the online BSA E-Filing System (<http://bsaefiling.fincen.treas.gov>). The Organization should already have an account set up on the BSA E-Filing System.
* <*If a banking financial institution*> If it is determined that a qualifying computer security incident has occurred, the primary regulator should be notified as soon as possible, but no later than 36 hours after the event. A qualifying computer security incident is an incident that has materially affected or is reasonably likely to materially affect the viability of operations, its ability to deliver banking products and services, or the stability of the financial sector.
* *<If a non-banking financial institution>* If it is discovered that a security breach involves the information of at least 500 consumers, the FTC should be notified as soon as possible, and no later than 30 days after discovery.
* <*If a higher education institution*> If required, the Federal Student Aid office can be notified of a breach using the Cybersecurity Intake Form (<https://fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity>).
* *<Incorporate any additional notification requirements that could impact your Organization>*
 |

### Closure (All Catalysts)

1. After the recovery and notification stages are complete, the IRT members should compile and organize the incident documentation.
2. The documentation will be analyzed to assess the incident damage and whether any financial loss to the Organization has occurred.
3. Any forensic evidence will be retained in a secure area until the evidence is no longer needed. It is imperative that the evidence is not tampered with so that the integrity of the evidence is maintained for future forensic testing and/or for legal purposes.
4. The IRT will meet to discuss the incident and determine what needs to be done differently in the future and what was learned from the experience.
5. A lawyer will be retained if any legal action is held against the Organization or if the Organization carries out legal action against the catalyst.
6. Necessary changes to the Organization’s policies and operating procedures should be made immediately and reported back to the IT Committee and sent to the Board for approval if necessary.
7. A final summary of the event will be presented to the IT Committee and <*Board of Directors or Board of Trustees*>. The Incident Summary Form in **Appendix D** will be used to document the incident.

*<The areas noted below should be updated to reflect applicable risks and threats to and mitigating controls, policies, and procedures in place at your organization.*

# Appendix A – Risk Assessment Documentation

## Threat Risk Assessment

| **Threat or Risk** | **Likelihood** | **Vulnerability** | **Potential Impact** | **Risk Rating** | **Controls in Place** | **Residual Risk** |
| --- | --- | --- | --- | --- | --- | --- |
| **Natural disaster** (floods, hurricanes, tornados, etc.) | Example rating: High | Locations are in areas that are prone to natural disasters | **Example rating: High*** Destruction or inaccessibility of equipment
* Locations become damaged or inaccessible to constituents
* Data lines become unavailable
* Loss of information and data
 | Example rating: High | * Locations are geographically spaced apart and constituents could be redirected to alternate sites
* Locations have redundant Internet connections and can operate independently
* Redundant data connection to the primary service provider
* Critical data is backed up and replicated
* The Organization’s primary services can be accessed remotely
* Business Continuity and Disaster Recovery (BC/DR) Plan includes procedures for operations and allows for employees to work remotely
* Insurance coverage is reviewed annually for adequacy
 | Example rating: Low |
| **Pandemic breakout** | <*insert rating*> | Building may be outside of “quarantine” area for several constituents | **<*insert rating*>*** Constituents may not be able to visit locations due to illness
 | <*insert rating*> | * Locations are geographically spaced apart and constituents could be redirected to alternate sites
* The Organization’s primary services can be accessed remotely
* BC/DR Plan includes procedures for operations and allows for employees to work remotely
 | <*insert*> |
| Employee shortage due to illness or quarantine | **<*insert rating*>*** Limited staffing
 | <*insert rating*> | <*insert*> |
| **Man-made disaster** (fire, chemical, liquid, leakage, explosion, etc.) | <*insert rating*> | Locations are in areas that are at risk for being completely or partially destroyed | **<*insert rating*>*** Destruction or inaccessibility of equipment
* Locations become damaged or inaccessible to constituents
* Data lines become unavailable
* Loss of information and data
 | <*insert rating*> | * Fire protection and suppression systems in place
* Locations are geographically spaced apart and constituents could be redirected to alternate sites
* Locations have redundant Internet connections and can operate independently
* Redundant data connection to the primary service provider
* Critical data is backed up and replicated
* The Organization’s primary services can be accessed remotely
* BC/DR Plan includes procedures for operations and allows for employees to work remotely
* Insurance coverage is reviewed annually for adequacy
 | <*insert*> |

| **Civil unrest** | <*insert rating*> | Local infrastructure may be weakened and building access unavailable | **<*insert rating*>*** Constituents not able to visit locations due to road closures or crowds
 | <*insert rating*> | * Locations are geographically spaced apart and constituents could be redirected to alternate sites
* Locations have redundant Internet connections and can operate independently
* Redundant data connection to the primary service provider
* Critical data is backed up and replicated
* BC/DR Plan includes procedures for operations and allows for employees to work remotely
* The Organization’s primary services can be accessed remotely
* Insurance coverage is reviewed annually for adequacy
 | <*insert*> |
| --- | --- | --- | --- | --- | --- | --- |
| Unrest escalation causing damage to locations and equipment | **<*insert rating*>*** Destruction or inaccessibility of equipment
* Locations become damaged or inaccessible to constituents
 | <*insert rating*> | <*insert*> |
| **Power failure** | <*insert rating*> | All operations depend on equipment (servers, workstations, etc.) | **<*insert rating*>*** Employees will not be able to perform basic duties without servers and workstations
 | <*insert rating*> | * Each location has a generator that is tested *<weekly>*
* Systems are equipped with power protection that allows limited time for emergency save and shutdown
* Redundant data connection to the primary service provider
 | <*insert*> |
| Main Office has the primary connection to primary service provider | **<*insert rating*>*** No location will be able to access primary service provider
 | <*insert rating*> | <*insert*> |
| Accidental loss of data that is currently being accessed | **<*insert rating*>*** Data keyed prior to save would be lost
 | <*insert rating*> | <*insert*> |
| **Equipment failure** | <*insert rating*> | Loss or corruption of data | **<*insert rating*>*** Data on failed equipment will be lost, corrupted, or unusable
 | <*insert rating*> | * Locations have redundant Internet connections and can operate independently
* Redundant data connection to the primary service provider
* Alternate systems are available for temporary use until replacement machines are reordered
* Default storage folders are mapped to server shares and minimal data should be stored locally on systems
* Critical data is backed up and replicated
* Procedures are in place for reordering IT equipment
* Redundant servers exist, which decreases the urgency for sever replacement
* Majority of servers are virtualized and can be quickly recreated
* Workstations can easily be ordered and replaced quickly
* Majority of applications are outsourced, and the vendor has appropriate backup procedures in place
* Non-outsourced applications are server-based and dependency on a single workstation is limited
* BC/DR Plan includes procedures for operations and allows for employees to work remotely
* Support and maintenance agreements are maintained
* IT support vendors are available and will be utilized
* Insurance coverage is reviewed annually for adequacy
 | <*insert*> |
| IT infrastructure will not be available | **<*insert rating*>*** Alternate locations cannot connect to primary location for file servers or access to the primary service provider
 | <*insert rating*> | <*insert*> |
| Workstations will not be available | **<*insert rating*>*** Employees will not to be able to perform daily job responsibilities
 | <*insert rating*> | <*insert*> |
| Servers will not be available | **<*insert rating*>*** Server will not provide designated services
 | <*insert rating*> | <*insert*> |
| Resources to restore system and infrastructure may be limited | **<*insert rating*>*** IT Department staffing is limited so the available resources to restore equipment may be limited
 | <*insert rating*> | <*insert*> |
| **Physical theft of data** (paper or electronic format) | <*insert rating>* | Data is stored on paper, electronic media, and computer equipment | **<*insert rating*>*** Data on the stolen format will no longer be available
 | <*insert rating*> | * Employees and contractors undergo background checks
* Employees and contractors sign confidentiality agreements
* Documents and electronic media marked for destruction are properly secured until shredded, destroyed, or wiped
* Electronic media (e.g., hard drives, DVDs, CDs, removable media) is limited using *<insert system>,* and authorized media is encrypted when utilized
* Incident Response Procedures exist
* Original paper documents are scanned immediately and stored in secured locations if retained
* Default storage folders are mapped to server shares and minimal data should be stored locally on systems
* Critical data is backed up and replicated
* Critical equipment is in locked areas with video surveillance and monitored alarm systems
 | <*insert*> |
| Data includes confidential information | **<*insert rating*>*** Compromise of confidential information
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating*> | <*insert*> |
| **Physical break-in** | <*insert rating*> | Locations and/or computer equipment could be destroyed | **<*insert rating*>*** Equipment could be destroyed or become inaccessible
* Locations could be damaged or inaccessible to constituents
 | <*insert rating*> | * Alternate systems are available for temporary use until replacement machines are reordered
* Procedures are in place for reordering IT equipment
* Redundant servers exist, which decreases the urgency for sever replacement
* Majority of servers are virtualized and can be quickly recreated
* Workstations can easily be ordered and replaced quickly
* Majority of applications are outsourced, and the vendor has appropriate backup procedures in place
* Non-outsourced applications are server-based and dependency on a single workstation is limited
* BC/DR Plan includes procedures for operations
* Support and maintenance agreements are maintained
* Insurance coverage is reviewed annually for adequacy
* Default storage folders are mapped to server shares and minimal data should be stored locally on systems
* Documents and electronic media marked for destruction are properly secured until shredded, destroyed, or wiped
* Electronic media (e.g., hard drives, DVDs, CDs, removable media) is limited using *<insert system>* and authorized media is encrypted when utilized
* Incident Response Procedures exist
* Original paper documents are scanned immediately and stored in secured locations if retained
* Default storage folders are mapped to server shares and minimal data should be stored locally on systems
* Critical data is backed up and replicated
* Critical equipment is in locked areas with video surveillance and monitored alarm systems
* Controls such as unique usernames, password and account lockout settings, inactivity timeouts, and multi-factor authentication are configured on applications and systems
* Constituents will be redirected to alternate locations
* Passwords are not written down in unsecure locations
 | <*insert*> |
| Equipment that is stolen could contain data that does not exist in any other format | **<*insert rating*>*** Data on the stolen equipment will no longer be available
 | <*insert rating*> | <*insert*> |
| Unauthorized access to constituent or Organization information  | **<*insert rating*>*** Confidential information may be compromised
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating*> | <*insert*> |
| **External electronic intrusion** | <*insert rating*> | Unauthorized access to constituent or Organization information | **<*insert rating*>*** Confidential information may be compromised
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating*> | * Annual vulnerability and penetration testing performed
* Malware protection is in place on systems, periodic scans are configured, and the anti-malware console is reviewed regularly
* Firewalls exist for ISP connections and are equipped with IDS/IPS features that are monitored 24x7 by *<insert name/vendor >*
* Network equipment (e.g., switches, routers, firewalls) and peripheral devices (e.g., Internet of Things devices, multi-function printers, copiers, scanners) are updated timely
* Patch management of servers, workstations, and laptops is centralized using *<insert system name>,* and the console is monitored regularly to ensure all devices are updated
* Unnecessary ports are closed on all networking firewalls
* Wireless access points are on segregated network, SSIDs are configured to not broadcast, and WPA2 encryption and a strong security key that is changed periodically are utilized
* Locations are interconnected via encrypted data lines
* Controls such as unique usernames, password and account lockout settings, inactivity timeouts, and multi-factor authentication are configured on applications and systems
* Default storage folders are mapped to server shares and minimal data should be stored locally on systems
* Critical data is backed up and replicated
* Majority of applications are outsourced, and the vendor has appropriate backup procedures in place
* Email encryption is utilized for sending confidential information
* Incident response procedures exist and include procedures for addressing zero-day vulnerabilities
 | <*insert*> |
| Loss or corruption of constituent or Organization information | **<*insert rating*>*** Data will be lost, corrupted, or unusable
 | <*insert rating*> | <*insert*> |
| **Malware** (virus, spyware, ransomware, etc.) | <*insert rating*> | Unauthorized access to constituent or Organization information | **<*insert rating*>*** Confidential information may be compromised
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating>* | * Annual vulnerability and penetration testing performed
* Malware protection is in place on systems, periodic scans are configured, and the anti-malware console is reviewed regularly
* Anti-ransomware protection is included in anti-malware product
* Anti-malware software installed on applicable mobile devices
* Firewalls exist for ISP connections and are equipped with IDS/IPS features that are monitored 24x7 by *<insert name/vendor >*
* Network equipment (e.g., switches, routers, firewalls) and peripheral devices (e.g., Internet of Things devices, multi-function printers, copiers, scanners) are updated timely
* Patch management of servers, workstations, and laptops is centralized using *<insert system name>,* and the console is monitored regularly to ensure all devices are updated
* Unnecessary ports are closed on all networking firewalls
* Network access is segmented to reduce the likelihood that the entire network is compromised by a single attack
* Controls such as unique usernames, password and account lockout settings, inactivity timeouts, and multi-factor authentication are configured on applications and systems
* Application whitelisting is used to prevent ransomware running
* Default storage folders are mapped to server shares and minimal data should be stored locally on systems
* Critical data is backed up and replicated, and the backups are not connected to the systems they are backing up (critical for ransomware scenarios)
* Majority of applications are outsourced, and the vendor has appropriate backup procedures in place
* Incident response procedures exist
* Electronic media (e.g., hard drives, DVDs, CDs, removable media) is limited using *<insert system>* and authorized media is encrypted when utilized
* Spam filtering is in place to prevent spread of malware via email, and addresses of known spammers and emails with executables are blocked
* Support and maintenance agreements maintained
* Employee information security training is conducted annually
* Web filtering prevents access to risky websites
 | <*insert*> |
| Loss or corruption of constituent or Organization information | **<*insert rating*>*** Data will be lost, corrupted, or unusable
 | <*insert rating*> |
| <*insert*> |
| **Employee fraud** | <*insert rating*> | Employee disclosure of confidential information to unauthorized source | **<*insert rating*>*** Unauthorized individuals will have confidential information
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating*> | * Employees undergo background checks
* Employees sign confidentiality agreements
* Annual employee training on privacy and confidentiality policies
* Each user is assigned a unique user account with minimum access rights to complete job functions
* Activity reports for <*the network, Active Directory, and other high-risk systems*> are reviewed by independent parties to identify suspicious activity
* Incident Response Procedures exist
 | <*insert*> |
| Unauthorized access to confidential information | **<*insert rating*>*** Employees access confidential constituent or Organization data and begin fraudulent behaviors
 | <*insert rating*> | <*insert*> |
| **Employee error** | <*insert rating*> | Accidental loss or corruption of confidential information | **<*insert rating*>*** Data will be lost, corrupted, or unusable
 | <*insert rating*> | * Annual employee training on privacy and confidentiality policies
* Malware protection is in place on systems, periodic scans are configured, and the anti-malware console is reviewed regularly
* Default storage folders are mapped to server shares and minimal data should be stored locally on systems
* Critical data is backed up and replicated
* Majority of applications are outsourced, and the vendor has appropriate backup procedures in place
* Incident response procedures exist
* Electronic media (e.g., hard drives, DVDs, CDs, removable media) is limited using *<insert system>* and authorized media is encrypted when utilized
* Spam filtering is in place to prevent spread of malware via email
* Employee information security training is conducted annually
* Web filtering prevents access to high-risk websites
 | <*insert*> |
| Accidental disclosure of confidential information | **<*insert rating*>*** Unauthorized individuals will have confidential information
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating*> | <*insert*> |
| Victim of spam or phishing resulting in malware or disclosure of information to unauthorized source | **<*insert rating*>*** Confidential information may be compromised
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating*> | <*insert*> |
| **Vendor failure** | <*insert rating*> | Accidental loss or corruption of data | **<*insert rating*>*** Data will be lost, corrupted, or unusable
 | <*insert rating*> | * If a breach or potential breach occurs, vendor has procedures to notify the Organization timely
* Vendors are not authorized to share constituent information with any third party unless specifically stated in contract
* Contracts include confidentiality, IT security, and breach notification clauses
* Vendors have appropriate security controls in place
* Vendors create daily backups with a strong retention schedule
* Vendors have disaster recovery procedures in place to provide a redundant system if their primary system is unavailable
* BC/DR Plan provides for temporary manual operations
* Vendor oversight procedures include reviewing documentation regarding information security, cybersecurity, business continuity and disaster recovery, insurance, etc.
 | <*insert*> |
| Accidental disclosure of data | **<*insert rating*>*** Unauthorized individuals will have confidential information
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating*> | <*insert*> |
| Not accessible | **<*insert rating*>*** Daily operations dependent on system that vendor provides will not be accomplishable
 | <*insert rating*> | <*insert*> |
| Security incident | **<*insert rating*>*** Unauthorized individuals will have confidential information
* Constituents, regulatory bodies, and authorities must be notified
 | <*insert rating*> | <*insert*> |
| **Constituent issue** | <*insert rating*> | Constituent impersonated (voice, in-person, email) | **<*insert rating*>*** Employee will perform transactions for unauthorized constituents
 | <*insert rating*> | * Employees are trained on procedures for verifying constituents in person, over the phone, and via mail, email, and fax
* Additional verification (e.g., call-back procedures) are performed for suspicious requests or high-risk transactions
* Constituent education programs have been developed to educate constituents on information security practices
* Multi-factor authentication implemented for high-risk systems
* Refer to the <*insert additional applicable policies and risk assessments*> for documentation of additional controls related to authentication, transactions, and identifying suspicious activity.
 | <*insert*> |
| Constituent has malware, which makes him vulnerable to identity theft, account takeover, or social engineering | **<*insert rating*>*** Constituent credentials could be stolen
* Confidential identification information could be obtained to impersonate the individual
 | <*insert rating*> | <*insert*> |
| **Social networking** | <*insert rating*> | Constituents post negative comments, sensitive information, or information that is not in compliance with laws and regulations | **<*insert rating*>*** Negative comments will be posted about the Organization
* Negative feedback may impact the Organization’s reputation
* Sensitive information could be released
* Constituent is susceptible to identity theft
* Postings make Organization liable to fines, lawsuits, etc.
 | <*insert rating*> | * Employees are trained on and sign the <*Acceptable Use Policy*>, which dictates acceptable use of social media
* Official pages registered on various site
* Login credentials to social media accounts restricted to certain staff, and strong passwords are utilized and changed frequently
* Policies and procedures exist to review postings for compliance with applicable consumer protection laws and regulations
* Incident response procedures address public postings of confidential or sensitive information
* Procedures address postings from unsatisfied constituents
* Periodic reviews are performed to identify fraudulent pages
* Privacy policies, as required by the Gramm-Leach-Bliley Act, are referenced on official pages
* Severe disciplinary actions exist for an employee’s or contractor’s posting of sensitive or confidential information
* Periodic monitoring and reporting to Management regarding employee usage during work hours
* Web filtering blocks unnecessary access to social media sites
* Refer to the <*insert social media policy name*> for further assessment of risks and controls
 | <*insert*> |
| Fraudulent pages posted on behalf of the Organization | **<*insert rating*>*** Organization unaware of postings made
 | <*insert rating*> | <*insert*> |
| Unrestricted access for employee usage | **<*insert rating*>*** Employee productivity decreases
 | <*insert rating*> | <*insert*> |

## Asset Risk Assessment

Below is a sample line item for the Asset Risk Assessment. This sample includes suggested controls that are relevant to many systems. This sample exists to show how assets can be incorporated into the risk assessment process. The sample should be edited to fully reflect the risks and controls associated with each asset. Ideally, all applications and technology systems that have a login or a management console or are critical assets to operations should be incorporated. Some assets that could be utilized by your organization include the following:

**All organizations**

* Accounting system
* Internet banking
* Anti-virus console
* Backup console
* Check writing
* Client management system
* Data analytics
* Email, email encryption, web mail portals
* End-user systems
* File transfer
* Firewall, intrusion detection and/or prevention system, and associated consoles
* Helpdesk
* Internal traffic monitoring
* Mobile device management
* Mobile devices
* Network (e.g., Active Directory, Open Directory)
* Patch management console
* Payroll
* Remote access via web applications (e.g., GoToMyPC, LogMeIn, Join.me) or VPN
* Scheduling
* Secure file sharing
* Servers (e.g., virtual, ESX, physical)
* Social networking sites (e.g., Facebook, Instagram, Twitter)
* Switches (management console)
* System utilized for DNS record management
* Virtualization
* VoIP management console
* Website management
* Wireless access management console

**Education**

* Online payments
* Learning management system
* Recruitment
* Student financial aid
* Student information system

**Medical**

* Electronic medical records
* Medical device management console

**Not-for-profit**

* Church management system
* Donor management

**Financial services/institutions**

* ACH (origination and receipt)
* ATMs, including management console
* ATM/debit cards
* Bill payment
* Branch capture and item processing
* Business remote deposit capture
* Check imaging
* Check ordering
* COLD/report storage
* Core system
* Correspondent financial institutions
* Credit cards
* Credit reporting
* Deposit platform and documentation
* Document imaging and archival storage
* eStatements
* Gift cards
* Internet banking
* Investments
* Loan platform and documentation
* Mobile banking
* Mortgage
* Person-to-person payments (P2P)
* Retail or mobile remote deposit capture
* Telephone banking
* Teller platform
* Trust service

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset or Application** | **Purpose** | **Data Classification** | **Vulnerability** | **Likelihood** | **Impact** | **Business Risk Rating** | **Controls in Place** | **Residual Risk** |
| *<For each application or technology asset, include applicable details about the system, vendor, etc.>*  | *<For each item, insert details of the purpose of the item.>* | *<List the classification of data (e.g., confidential, sensitive, public) stored or accessed by each asset.>* | Unauthorized data access by constituent, hacker, or other outsider or physical theft of server and data storage | <*Insert*> | <*Insert*> | <*Insert*> | * Principle of least privilege applied when granting user access
* User access is reviewed <*annually*> to ensure access remains restricted
* Integration with Active Directory for authentication
* Complex passwords with a minimum of *<insert>* characters and complexity are enforced
* Passwords expire after *<insert>* days, and the last *<insert>* passwords cannot be reused
* Accounts are locked after *<insert>* invalid attempts and require administrator reset
* Inactivity timeout activates after *<insert>* minutes
* Multi-factor authentication is enabled via *<token, text code, IP address restriction>*
* Password self-reset is allowed after a user answers a series of complex challenge questions, and a new temporary password is emailed to email address on file
* Administrative and service account passwords are known by few individuals and are changed at least annually
* Activity logging is configured and monitored by *<insert>* on a *<daily, weekly>* basis
* Data is encrypted in transit over external networks and at rest <*consider including details related to encryption capabilities and any transfers of data over external networks*>
* SSL certificate required
* VPN device in the DMZ
* Physical security controls are in place (e.g., firewall, IDS/IPS, IT Department, and Computer Room are physically restricted with access cards and key locks, video surveillance, etc.) (OR Vendor has extensive physical security controls in place)
* Web management consoles are disabled
* Updates are applied to the system when available to ensure devices are not vulnerable to unauthorized or remote access
* Email system automatically encrypts items containing attachments or messages that appear to contain Social Security Numbers or other PII
* Employees instructed on proper use of email system to ensure Organization or constituent data is not inadvertently sent to wrong individual
* System configured to never save password
* Policies, procedures, and training on acceptable use
* Users prohibited from accessing on public computers
* Wireless access points are segregated from data network; the SSID is not configured to broadcast; WPA2 encryption is utilized; the wireless key changes periodically; disabled when not in use; physical device is stored in a limited access area; broadcast range is limited within building
* Remote access for vendor sessions into the systems is initiated and approved internally by IT Department, and remote access sites are blocked by web filter
* Periodic review of workstations for unauthorized software
 | <*Insert*> |
| Data corruption or loss | <*Insert*> | <*Insert*> | <*Insert*> | * Data is backed up and replicated to multiple locations *<OR Vendor backs up and replicates to multiple locations>*, including *<insert>*
* The following data retention period has been established: *<10 daily, 4 EOW, 12 EOM, 3 EOY>*
* *<Insert>* monitors backup status reports daily to identify and resolve potential issues
* Original hard copy documentation is retained for *<insert>* days
* File transfer systems are not used for storage of critical data, and data requiring backup is stored on servers that are backed up
 | <*Insert>* |
| Vendor breach | <*Insert*> | <*Insert*> | <*Insert*> | * Vendor has appropriate security controls, redundancy, and breach notification procedures, and these are reviewed in the annual vendor review. <*Include applicable details.*>
 | <*Insert*> |
| Unavailability | <*Insert*> | <*Insert*> | <*Insert*> | * Backup agreement in place with *<insert>*
* Redundant data connection with vendor
* Locations have redundant Internet connections and can operate independently
* System can be accessed from any location with an Internet connection and there is minimal dependence on network
* Critical data is backed up and replicated to multiple locations
* Administrative passwords are stored in a secure area
* Customers can submit checks and/or make donations at a branch/office location
* Configurations for network equipment are backed up *<quarterly or any time changes are made>*
 | <*Insert*> |

*The following depicts a sample assessment for two applications (e.g., accounting system and Outlook Web Access) and several critical technology assets. This sample is for illustrative purposes only to depict how the sample above can be implemented.*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset or Application** | **Purpose** | **Data Classification** | **Vulnerability** | **Likelihood** | **Impact** | **Business Risk Rating** | **Controls in Place** | **Residual Risk** |
| Accounting System Online(ABC Vendor)*Data is hosted by ABC Vendor using Amazon Web Services* | Finance system, general ledger, payroll | Sensitive | Unauthorized data access or physical theft of server and data storage | <*Insert*> | <*Insert*> | <*Insert*> | * Principle of least privilege applied when granting user access
* User accounts and access rights reviewed annually performed by the CFO to ensure access remains appropriately restricted
* Complex passwords are enforced by system
	+ Minimum of 8 characters
	+ Must include letter, number, and special character
	+ Expiration of 45 days with history of 10 passwords
* Accounts are locked after 3 invalid attempts and the user must be reset by an administrator (password self-reset is not allowed)
* Inactivity timeout activates after 10 minutes of inactivity
* Multi-factor authentication is enabled using token authentication, and IP address restrictions are configured to the internal network or pre-approved wireless cards
* Administrator and service account passwords are known only by the CFO and IT Department and are changed annually
* Activity logging is configured, and system alerts *<insert>* via email of suspicious activity requiring investigation
* Data is hosted at Amazon Web Services, which is a hardened facility with extensive physical security controls in place. All data is encrypted at rest at the database level and server level.
* Data from this system is transferred to XYZ system and the transfer is encrypted
 | <*Insert*> |
| Data corruption or loss | <*Insert*> | <*Insert*> | <*Insert*> | * ABC Vendor utilizes Amazon Web Services to host data, and data is replicated between Site A and Site B on an hourly basis
* ABC Vendor backs up data according to the following retention schedule: *<2 weeks daily, 4 EOW, 12 EOM, 3 EOY>*
* <*insert*> monitors backup status reports weekly
 | <*Insert*> |
| Vendor breach | <*Insert*> | <*Insert*> | <*Insert*> | * ABC Vendor has appropriate security controls, redundancy, and breach notification procedures, which are reviewed annually
 | <*Insert*> |
| Unavailability | <*Insert*> | <*Insert*> | <*Insert*> | * Locations have redundant Internet connections and can operate independently. This system can be accessed from any internal location with an Internet connection.
* Data is backed up and replicated to multiple data centers
* Administrative passwords stored in a secure area
 | <*Insert*> |
| Outlook Web Access (OWA)Internally hosted Exchange servers | Web mail | Sensitive | Unauthorized data access or physical theft of server and data storage | <*Insert*> | <*Insert*> | <*Insert*> | * OWA enabled only for Management and C-level employees
* User accounts and access rights are reviewed by <*insert*> quarterly to ensure access remains appropriately restricted
* The system integrates with Active Directory for authentication, and complex passwords are enforced by Active Directory
	+ Minimum of 10 characters
	+ Must include letter, number, and special character
	+ Expiration of 90 days with history of 10 passwords
* Accounts are locked after 3 invalid attempts and the user must be reset by an administrator (password self-reset not allowed)
* Inactivity timeout activates after 10 minutes
* Multi-factor authentication is enabled using a code sent by text or voice to the phone number on file
* Administrator and service account passwords are known by the IT Department and are changed annually
* System is configured to never save password
* Policies, procedures, and employee training on acceptable use
* Employees prohibited from accessing on public computers
 | <*Insert*> |
|  |  | Data corruption or loss | <*Insert*> | <*Insert*> | <*Insert*> | * Email is not to be utilized for storing critical data, so the risk of data corruption or loss is minimal
 | <*Insert*> |
|  |  | Unavailability | <*Insert*> | <*Insert*> | <*Insert*> | * Locations have redundant Internet connections and can operate independently. This system can be accessed from any location with an Internet connection.
* Administrative passwords stored in a secure area
 | <*Insert*> |
| Mobile devices | Accessing network resources | Sensitive | Unauthorized data access or physical theft | <*Insert*> | <*Insert*> | <*Insert*> | * Mobile Device Acceptable Use Policy signed by all employees and annual training provided on acceptable usage
* Management software has been implemented to centrally manage devices, and the following controls are enforced
	+ 6-digit PIN that must change annually
	+ Device locks after no more than 5 minutes
	+ Remote wipe capabilities if device is lost or stolen
	+ Containerization implemented for Organization data
	+ Hard drive encryption (native to device or installed)
	+ Anti-malware software required for applicable systems
	+ Updates applied within one month of release
	+ Data storage restrictions
 | <*Insert*> |
| ATMs | Cash withdrawal | Confidential | Unauthorized data access by employee, hacker, or outsider or physical theft of server/data storage | <*Insert*> | <*Insert*> | <*Insert*> | * ATMs are located on a separate VLAN from main network
* Vendor maintains ATM network and ATMs and applies necessary patches and updates
* Physical security in place, including firewall and IDS
* Anti-malware software installed
* Daily physical inspection for tampering (e.g., skimming devices)
* Confidentiality agreement in place with ATM vendor
* Complex passwords are required for management
	+ Minimum of 8 characters
	+ Must include letter, number, and special character
	+ Expiration of 45 days with history of 10 passwords
 | <*Insert*> |
| Data corruption or loss | <*Insert*> | <*Insert*> | <*Insert*> | * Vendor backs up data daily and retains daily backups for two weeks. EOM backups are retained for 12 months.
 | <*Insert*> |
| Unavailability | <*Insert*> | <*Insert*> | <*Insert*> | * Tellers can serve customers for cash transactions
 | <*Insert*> |
| End-user systems | Desktops, thin clients, laptops | Confidential | Unauthorized data access | <*Insert*> | <*Insert*> | <*Insert*> | * Domain user accounts utilized instead of local user accounts and password and account lockout group policies apply
* Screensaver timeout activates after 15 minutes of inactivity
* Patching and anti-malware update procedures in place
* ‘Administrator’ and ‘Guest’ accounts disabled
* Passwords are not written down in non-secure locations
* Employees are not authorized to install applications
* Annual information security training conducted
* Web filtering prevents access to high-risk websites
* Removable media blocked using *<insert>*
* Devices are easily replaceable
* Default storage folders are mapped to server shares and minimal data should be stored locally to increase likelihood that critical data is backed up and replicated
* Firewall and IDS/IPS in place and monitored 24x7
 | <*Insert*> |
| Data corruption or loss | <*Insert*> | <*Insert*> | <*Insert*> | <*Insert*> |
| Unavailability | <*Insert*> | <*Insert*> | <*Insert*> | <*Insert*> |
| VoIP | Voice-over-IP | Sensitive | Unauthorized data access | <*Insert*> | <*Insert*> | <*Insert*> | * Physical security over servers and monitored firewall/IDS
* Complex passwords required and must have 8 characters with letter and number, 1 special character, and be changed every 45 days with a password history of 10 passwords
* Data encryption of all calls
* Auditing of user sessions and administrative activities
 | <*Insert*> |
| Spamming Over Internet Telephony (SPIT) | <*Insert*> | <*Insert*> | <*Insert*> | * Blacklisting approach utilized to block known spam addresses
 | <*Insert*> |
| Unavailability | <*Insert*> | <*Insert*> | <*Insert*> | * Emergency calls rerouted appropriately
* Analog line maintained
 | <*Insert*> |
| Identity and service theft (e.g., eavesdropping, phreaking, vishing) | <*Insert*> | <*Insert*> | <*Insert*> | * Encryption of calls
* Regular review of phone bills and charges
* Employee training on social engineering attacks
* Whitelisting of callable country codes
 | <*Insert*> |

# Appendix B – Vendor Relationship Management

## Vendor Relationship Inventory

*<Use this table to maintain an inventory of all vendor relationships.>*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Vendor** | **Relationship Owner** | **Description of Service** | **Contract Term, Renewal, and Expiration Date** | **Has Regular Access to Constituent Data or Access to Network** | **Vendor Classification** | **Last Review Date** | **Management Decision**  |
| *<Insert applicable vendors>* | *<Insert staff member or position>* | *<Insert services, systems, or functions provided>.* |  |  | *Ex: Critical, Significant, or Non-Critical* |  | *Ex: Continue, Modify, or Terminate* |
| Example:Vendor 1 | CFO | Hosting of QuickBooks for accounting and finance |  | No | Critical | 1/2020 | Continue |
| Example: Vendor 2 | CFO | Hosting of donor management system |  | Yes, donor details | Critical | 1/2020 | Continue |
| Example: Vendor 3 | Facilities Officer | Janitorial and shredding services |  | Potential access to physical data and systems | Non-Critical | 1/2018 | Continue |
| Example: Vendor 4 | ISO | Intrusion detection monitoring |  | No | Significant | 1/2019 | Continue |
| Example: Vendor 5 | IT Manager | Network support |  | No direct access to data but 24x7 remote network access | Critical | 1/2020 | Reevaluate due to lack of assurance related to security controls |

##

## New Product / Vendor Evaluation Form

|  |  |
| --- | --- |
| **Procedure** | **Notes** |
| **General Information** |
| Summary of product or service |  |
| Proposed vendor(s) |  |
| Review date |  |
| Individual(s) performing the review |  |
| Date review documentation and contract presented to Management |  |
| Date regulator notification provided (for financial institutions)  |  |
| Date of relevant policy updates  | *<Consider risk assessments, IS Program, IT Policy, Incident Response, Business Continuity and Disaster Recovery, etc.>* |
| **Relationship to Strategic Plan** |
| *
 |
| **Benefits** |
| *
 |
| **System/Data Hosting**  |
| *
 |
| **Costs** |
| *
 |
| **Potential Compliance, Privacy and/or Legal Issues** |
| *
 |
| **Target Implementation Timeframe** |
| *
 |

**Risk Assessment of Technology**

The following summary of risks has been created to identify inherent risks associated with the proposed new product or service. The probability and impact of each risk has been assessed. Control measures will be warranted for all medium or high probability and impact ratings. The following types of risks have been considered: strategic risk, reputation risk, operational risk, transaction risk, credit risk, compliance, and other miscellaneous risks.

Residual risk represents the risk(s) that are still present once controls have been implemented. Management will aim to always have a very low residual risk.

|  |  |  |  |
| --- | --- | --- | --- |
| **Inherent Risks Identified** | **Probability** | **Impact** | **Controls to Be Utilized** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Summary of Residual Risk Level** |
|  |

**Vendor Evaluation**

The following list contains many items that may be reviewed and analyzed as part of due diligence procedures.

|  |  |  |
| --- | --- | --- |
| **Completed** | **Item Reviewed** | **Responses and Notes** |
|  | Audited financial statements, annual reports, SEC filings, and other available financial indicators |  |
|  | Experience and ability to implement and monitor the proposed activity |  |
|  | Experience and ability in implementing and monitoring the proposed activity |  |
|  | Business reputation, status in the industry, and sustainability  |  |
|  | Qualifications, training, and experience of the company’s principals and staff |  |
|  | Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies |  |
|  | Existence of significant complaints, litigation, or regulatory actions against the company |  |
|  | Ability to perform the proposed functions using current systems or the need to make additional investments |  |
|  | Use of other parties or subcontractors  |  |
|  | Scope of internal controls, information security (systems and data security), privacy protections, and audit coverage (vulnerability testing) |  |
|  | Business resumption strategy and contingency plans (to include pandemic planning and relevant threats such as DDoS) |  |
|  | Adequacy of data security policies (to include location, encryption, segregation, end-user logical access controls, and recovery information)  |  |
|  | Knowledge of relevant consumer protection regulations and civil rights laws  |  |
|  | Adequacy of management of information systems |  |
|  | Insurance coverage (focus on cybersecurity preparedness)  |   |
|  | Eligibility to perform as a service provider given the existence of any outstanding enforcement actions against the third party and the requirements of Section 19 of the FDI Act that may apply to Organization-affiliated parties |  |
|  | Record retention and maintenance practices  |  |
|  | Identification of potential conflicts of interest |  |
|  | Impact of proposed contracts on the third party’s operations and financial condition |  |

**Vendor Contract Review**

The Organization’s legal counsel will review all major contracts for the following items before the contract is approved by the <*Board of Directors or Board of Trustees*> and signed by Management. For minor contracts, the review will be performed internally.

|  |  |  |
| --- | --- | --- |
| **Item Confirmed** | **Contract Item** | **Responses and Notes** |
| **Contract Scope** |
|  | Timeframe covered by the contract is appropriate |  |
|  | Frequency, format, and specifications of the service or product to be provided are defined |  |
|  | Other services to be provided by the third party, such as software support and maintenance, training of employees, distribution of required disclosures to Organization’s constituents, and constituent service are clearly defined |  |
|  | Requirement that third party is required to comply with all applicable laws, regulations, and regulatory guidance is addressed  |  |
|  | Contract authorizes the Organization and the appropriate federal and state regulators to have access to records of the third party as necessary or appropriate to evaluate compliance with laws, rules, and regulations |  |
|  | Contract identifies which party will be responsible for delivering any required constituent disclosures |  |
|  | Contract requires third party to maintain appropriate insurance coverage  |  |
|  | Contract identifies terms relating to any use of Organization premises, equipment, or employees |  |
|  | Contract includes appropriate permissibility or prohibition of the third party to subcontract or use another party to meet its obligations with respect to the contract and any notice or approval requirements**Note**: Any material contract should prohibit assignment, transfer, or subcontracting to another entity, unless and until the Organization determines that such assignment, transfer, or subcontract would be consistent with the due diligence standards  |  |
|  | Contract includes authorization for the Organization to monitor and periodically review the third party for compliance with its agreement |  |
| **Cost/Compensation Issues Outlined** |
|  | The fees to be paid, including any fixed compensation, variable charges, and fees to be paid for nonrecurring items or special requests are identified |  |
|  | Cost and responsibility for purchasing and maintaining any equipment, hardware, software, or other item related to the activity are identified |  |
|  | Party responsible for payment of any legal or audit expenses is identified |  |
|  | Volume and short-term incentives have been analyzed and are subject to strict quality control *(This item is of concern in financial institutions with loan originations, and the FDIC expressly discourages the use of compensation arrangements which may encourage third-party originators to inappropriately steer borrowers into higher-cost products.)* |  |
| **Performance Standards** |
|  | Performance standards, including data availability, have been identified, if applicable |  |
|  | Adequate and measurable service level agreements (SLAs) are in place |  |
| **Reports** |
|  | The type and frequency of management information reports to be received has been specified (this may include performance reports, audits, financial reports, security reports, and business resumption testing reports) |  |
|  | Activity logs and reports can be provided in the event of inappropriate or illegal activity |  |
| **Audit** |
|  | The types and frequency of audit reports that the Organization is entitled to receive are identified |  |
|  | Contract specifies the Organization’s right to audit the third party (or engage an independent auditor) as needed |  |
|  | Costs, if any, for obtaining reports are identified |  |
| **Confidentiality and Security** |
|  | Contract acknowledges that the third party is responsible for the confidentiality and security of the Organization’s confidential data that it possesses, stores, processes, or transmits  |  |
|  | Contract stipulates that the third-party security controls are regularly reviewed and validated by an independent party  |  |
|  | Contract specifies that nonpublic personal information on the Organization’s constituents must be handled in a manner consistent with privacy policy and in accordance with applicable privacy laws and regulations |  |
|  | Contract specifies that any information security or business continuity incidents or breaches, including a potential breach resulting from an unauthorized intrusion, will be fully and promptly disclosed |  |
|  | Contract establishes responsibilities for responding to security events |  |
|  | Contract specifies that proper oversight of vendor employee access and client employee access is in place |  |
|  | Contract should guarantee transparency and proactive notification of system availability, production issues, scheduled downtime, and pending updates |  |
| **Constituent Complaints** |
|  | Contract specifies whether the Organization or the third party has duty to respond to complaints |  |
|  | If the third party is responsible for such responses, a copy of any complaint and the response should be forwarded to Organization |  |
|  | Contract provides for periodic summary reports detailing the status and resolution of complaints |  |
| **Business Resumption and Contingency Plans** |
|  | Contract addresses responsibility for service continuation in the event of operational failure, including both man-made and natural disasters |  |
|  | Contract addresses data replication location(s), schedule, and procedures for recovery and restoration |  |
|  | Costs for data retrieval have been identified |  |
|  | Results of testing of plans will be provided to the Organization |  |
| **Default and Termination** |
|  | Contract specifies what circumstances constitute default, identifies remedies, and allows for a reasonable opportunity to cure a default |  |
|  | Contract identifies the recourse available to the Organization should the third party fail to meet defined security requirements |  |
|  | Termination rights may be sought for various conditions, such as a change in control, substantial increase in cost, failure to meet performance standards, failure to fulfill contractual obligations, inability to prevent violations of law, bankruptcy, company closure, and insolvency |  |
|  | Return of the Organization’s data, records, and/or other resources is addressed, including any data migration and sanitization procedures |  |
|  | Exit or de-conversion costs and responsibilities are identified |  |
| **Dispute Resolution** |
|  | Details of dispute resolution process |  |
| **Ownership and License** |
|  | Contract addresses ownership issues and the third party’s right to use the Organization’s property, including data, equipment, software, and intellectual property such as the Organization’s name and logo, trademark, and other copyrighted material |  |
|  | Contract addresses ownership and control of any records generated by the third party |  |
| **Indemnification** |
|  | Indemnification provisions require a third party to hold the Organization harmless from liability because of negligence by third party (vice versa) |  |
|  | Indemnification or other compensation for contract violations  |  |
| **Limits on Liability** |
|  | The third party may wish to contractually limit the amount of liability incurred and Management has considered whether the proposed damage limitation is reasonable compared to the amount of loss the Organization could experience |  |

## Annual Vendor Review Checklist

|  |  |
| --- | --- |
| **Task** | **Notes** |
| **Vendor**  |  |
| **Review date** |  |
| **Review performed by** |  |
| **Recommended decision for vendor relationship** | Ex: continue as is, modification of XYZ, termination, and replacement  |
| **Information Security Program and other updates required (e.g., BC/DR, Incident Response, Information Technology)** |  |

|  |
| --- |
| **Contract review** |
| **Contract term (initial, renewal)** |  |
| **Termination requirements** |  |
| **Confidentiality clause**  |  |
| **Breach notification** |  |
| **Information security**  |  |
| **SLA requirements** |  |
| **Has vendor met SLA requirements noted above?** |  |
| **Subcontractor use considerations** |  |

*<Contract terms likely cannot be altered until renewal; however, completing this portion will assist you in remaining updated on the contract term, any termination or renewal requirements, and critical areas such as information security that may need to be incorporated into the contract upon future renewals.>*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Date requested** | **Date reviewed** | **Summary** | **Areas of Concern** |
| **Financial Viability** |
| **Audited financial statements, annual reports, SEC filings, and other available financial indicators**  |  |  |  |  |
| **Insurance coverage** |  |  |  |  |
| **Information Security Controls and Planning** |
| **Security audit report or controls assessment** *(ensure vulnerability testing performed)* |  |  |  |  |
| **Information security program** |  |  |  |  |
| **Oversight of vendors and third-party relationships** |  |  |  |  |
| **Foreign-based risks** |  |  |  |  |
| **Business Continuity and Disaster Recovery** |
| **Business continuity and disaster recovery plan** *(consider changes and updates and new threats such as DDoS and zero-day attacks)* |  |  |  |  |
| **Disaster recovery testing,** including integrated testing with the Organization’s plan |  |  |  |  |
| **Threat Identification, Issue Resolution, and Incident Response**  |
| **Cybersecurity resilience and preparedness**  |  |  |  |  |
| **Incident response** |  |  |  |  |
| **Summary of constituent complaint resolutions**  |  |  |  |  |
| **Breach identification, escalation, and notification procedures** |  |  |  |  |
| **Compliance Requirements** |
| **Regulatory examination report** *(financial institutions will request from primary regulator)* |  |  |  |  |
| **General procedures for compliance reporting** |  |  |  |  |
| **Identity theft program** |  |  |  |  |
| **Affiliate relationships (e.g., Federal Reserve Reg W)** |  |  |  |  |
| **Consumer compliance** |  |  |  |  |
| **PCI DSS requirements**  |  |  |  |  |
| **Other** |  |  |  |  |
| **Other** |
| **Performance standard reporting** |  |  |  |  |
| **Vendor awareness of emerging technologies** |  |  |  |  |
| **Onsite reviews** (if warranted after analysis) |  |  |  |  |
| **Other** |  |  |  |  |

## Confidentiality Agreement

Whereas *<insert Organization name here>* (hereinafter, the Organization) has contracted with \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to perform various functions or review on our behalf, and whereas, in order to perform this work, access to potentially confidential information and systems may be necessary, it is agreed that:

Confidential Information is information not generally known by the public including, but not limited to, the Organization’s (i) internal personnel, financial, marketing, and other proprietary business information, (ii) passwords to various systems within the Organization, (iii) computer equipment and resources and their peripheral equipment, (iv) access to secured locations such as the computer room, and (v) the Organization’s constituent base.

It is further acknowledged that except as expressly authorized in writing in advance by any party, either during the existence of this Agreement or at any time thereafter, parties shall not (i) copy or disclose Confidential Information to any third party except to its employees or consultants with a bona fide need to know the same in order to use the Confidential Information for the purposes of this Agreement, provided that such employees or consultants agree in writing prior to disclosure to the same obligations of confidentiality as those imposed on the parties hereunder with no further rights of disclosure, and provided that such disclosing party shall be responsible for the breach of such obligations by an such persons, or (ii) use Confidential Information for the benefit of anyone other than said party for the specific purpose of fulfilling said party’s obligations under this Agreement.

No Confidential Information can be at any time, directly or indirectly, authorized or disclosed regarding the Organization’s constituents or any of its operations.

This Agreement shall be binding upon and inure to the benefit of the successors, assignees, and legal representatives of the respective parties hereto.

In addition to any other remedies it may have, the Organization shall have the right to enforce this agreement by obtaining an injunction or specific performance from any court of competent jurisdiction.

If any term or provision of this agreement is held to be illegal, invalid, or unenforceable under the laws, regulations or ordinances of any federal, state, or local government, the remaining terms shall remain unaffected thereby. This agreement shall be constituted under the laws of Louisiana and venue shall be proper in Louisiana.

This instrument is executed on the day, month and year set forth below.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Printed Name  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Company |

# APPENDIX C – Cybersecurity Threat Log

<*This log can be utilized to track remediation of various cybersecurity threats and the efforts taken by the organization to mitigate.>*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Vulnerability** | **Affected Systems** | **Resolution** | **Status** |
| 00/00/2020 | Ex: zero-day vulnerability for Cisco router that allows for remote exploitation (CVE # ABC) | All Cisco routers | Weekly monitor for patch. Accepted risk of vulnerability until then because cannot disconnect from Internet due to reliance on device. Implemented additional endpoint monitoring to timely identify issues.  | Monitoring |
| 00/00/2020 | Ex: vulnerability associated with various versions of Microsoft | Microsoft versions ABC | Confirmed no systems affected. | Closed |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# appendix D – Incident Response Documentation

## Notice of Fraudulent Activity Letter

###

*<The following alerts can be utilized by financial institutions to alert other financial institutions of fraudulent origination files sent.>*

### Informal

A FRAUDULENT file was processed for **<INSERT ORGANIZATION NAME AND ABA>** in error on **<INSERT MM/DD/YY>**. The original file was processed on **<INSERT MM/DD/YY >** with settlement of **<INSERT MM/DD/YY >**. The FRAUDULENT file was processed on **<INSERT MM/DD/YY >** and will settle on **<INSERT MM/DD/YY >**. A reversal file was processed on **<INSERT MM/DD/YY >** and will settle on **<INSERT MM/DD/YY >**. For additional information, contact **<INSERT ORGANIZATION NAME>** at **<INSERT ORGANIZATION PHONE NUMBER>**.

**<INSERT ORGANIZATION NAME AND ABA>**hereby assumes all responsibility and liability for any processing errors, losses, damages, and liability in any way arising out of the transmission of the broadcast message. **<INSERT ORGANIZATION NAME AND ABA>**also agrees to indemnify and hold harmless the Federal Reserve Bank, its agents, and employees, from and against all claims, damages, lawsuits, and expenses, including reasonable attorneys’ fees, in any way arising out of the transmission of the broadcast message.

### Formal

A formal notice can be found on the following page.

This Agreement is made and entered into by and between <**INSERT RECEIVING ORGANIZATION NAME**> and **<INSERT YOUR ORGANIZATION NAME>** (the “Indemnifying Organization”) on <INSERT DATE> the following erroneous/improper/unauthorized transaction(s) occurred, resulting in funds being deposited at **<INSERT RECEIVING ORGANIZATION NAME>:**

Amount: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Funds”)

Constituent Name: Not known – name in file does not match name on the account

Account Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Account”)

The Indemnifying Organization hereby requests **<INSERT RECEIVING ORGANIZATION NAME>** to debit and/or place a hold on the Account to which the Funds were deposited for the amount deposited in error or the balance in the account if less than the original transaction amount and to remit said funds to the Indemnifying Organization and/or to hold funds in the Account pending further investigation.

The Indemnifying Organization hereby agrees that any decision to debit and/or place a hold on the Account is at the discretion of **<INSERT RECEIVING ORGANIZATION NAME>**. If **<INSERT RECEIVING ORGANIZATION NAME>** elects to hold the Funds in the Account and later makes a determination to release the Funds to the **<INSERT RECEIVING ORGANIZATION NAME>** customer, the terms of this Agreement are still in effect regardless of the Indemnifying Organization’s recovery or collection of Funds.

In consideration for **<INSERT RECEIVING ORGANIZATION NAME>** taking the actions requested in paragraph 2 of this Agreement, the Indemnifying Organization agrees to indemnify, defend and hold **<INSERT RECEIVING ORGANIZATION NAME>**, its officers, directors, employees, and agents, harmless against and from any and all losses, damages, liabilities, claims (including but not limited to third party claims), demands, suits, actions, proceedings, judgments, obligations, penalties, costs, or expenses including, without limitation, attorney fees, court costs, paid or incurred which arise directly or indirectly out of the holding and/or delivery of said funds to the Organization.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed and do each hereby warrant and represent that their respective signatories below have been and are on the dates listed below duly authorized by all necessary and appropriate corporate action to execute this Agreement.

Agreed to and Accepted By: Agreed to and Accepted By:

|  |  |
| --- | --- |
| **<INSERT YOUR ORGANIZATION NAME>** | **<INSERT RECEIVING ORGANIZATION NAME>** |
| (The “Indemnifying Organization”) |  |
| By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## Sample Constituent Alert Letter

**Important Notice of Unauthorized Access to Your Information**

You are receiving this notice because *<insert Organization name>* has become aware of an incident of unauthorized access to sensitive constituent information. Upon our immediate investigation, it has been determined that it is likely that this information has been or will be misused.

“Sensitive constituent information” is, by definition, a constituent’s name, address, or telephone number, in conjunction with his/her Social Security number, driver’s license number, account number (not limited to an account from which withdrawals or transfers can be made), credit or debit card number, or PIN or password that would permit access to the constituent’s account. It also includes any combination of components of constituent information that would allow someone to log onto or access the constituent’s account, such as user name and password or password and account number, including encrypted information.

Please note from the statement below that from our investigation**:**

*(One statement should be selected to indicate the results of the Organization’s investigation.)*

 We can determine from logs or other data precisely which constituents’ information has been improperly accessed and we can confirm that your information was compromised.

 We can determine that a group of files have been improperly accessed but we cannot identify which specific constituents’ information has been accessed. You are receiving this notice because your information is included in this group and may have been improperly accessed.

A description of the incident and the type of information that was subject to unauthorized access or misuse is as follows.

Please contact <*insert contact name*> at <*insert contact number*> or use our toll-free number at <*insert contact number*> for further information and assistance. Please refer to this notice when you call us.

Details of the steps we have taken to prevent any further unauthorized access of our constituent’s information are noted in the space below.

**What can you do to help fight identity theft?**

Review your account statements immediately and report any suspicious activity. Place a fraud alert on your credit bureau by contacting us or by contacting one of the three nationwide credit reporting agencies to put creditors on notice that you may be a victim of identity theft.

**What are fraud alerts?**

There are two types of fraud alerts: an initial alert and an extended alert.

An **initial alert** stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you’ve been taken in by a phishing scam. When you place an initial fraud alert on your credit report, you’re entitled to one free credit report from each of the three nationwide consumer reporting companies.

An **extended alert** stays on your credit report for seven years. You can have an extended alert placed on your credit report if you’ve been a victim of identity theft and you provide the consumer reporting company with an identity theft report. When you place an extended alert on your credit report, you’re entitled to two free credit reports within 12 months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre‑screened credit offers for five years unless you ask them to put your name back on the list before then.

To place either of these alerts on your credit report or to have them removed, contact one of the three major credit bureaus. You will be required to provide appropriate proof of your identity, which may include your SSN, name, address, and other personal information requested by the consumer reporting company. You may use a personal representative to place or remove an alert.

When a business sees the alert on your credit report, it must verify your identity before issuing credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you’re trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

**Equifax** - [www.equifax.com](http://www.equifax.com)
*To order your report*, call 800-685-1111 or write
P.O. Box 740241, Atlanta, GA 30374-0241

*For Fraud Alerts*, call 800-525-6285 and write
P.O. Box 105069, Atlanta, GA 30348-5069

Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.

**Experian** - [www.experian.com](http://www.experian.com)
*To order your report*, call 888-EXPERIAN (397-3742) or write
P.O. Box 2002, Allen, TX 75013

*For Fraud Alerts*, call 888-EXPERIAN (397-3742) and write
P.O. Box 9530, Allen, TX 75013
TDD: 1-800-972-0322

**Trans Union** - [www.transunion.com](http://www.transunion.com)
*To order your report*, call 800-888-4213 or write
P.O. Box 1000, Chester, PA 19022

*For Fraud Alerts*, call 800-680-7289 and write
Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834
TDD: 1-877-553-7803

We would like to remind you to be vigilant over the next 12 to 24 months and to always report incidents of suspected identity theft. You can file a complaint with the Federal Trade Commission (FTC) online at [www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-identity-theft) or call toll free 1-877-IDTHEFT (438-4338).

## Incident Summary Form

|  |  |
| --- | --- |
| **Procedure** | **Notes** |
| **Triage** |
| 1. Date of incident
 |  |
| 1. General description of incident
 |  |
| 1. Date/time of initial IRT meeting
 |  |
| 1. Initial IRT meeting notes
 |  |
| 1. How was the incident detected?
 |  |
| 1. Is the incident still in progress?
 |  |
| 1. Can the incident be quickly contained?
 |  |
| 1. What data or property is threatened?
 |  |
| 1. What system or systems are targeted and where are they located physically and on the network?
 |  |
| 1. What is the severity of the current or potential impact to the Organization?
 |  |
| 1. How critical are those assets to the ongoing operations of the Organization?
 |  |
| 1. Will the response alert the attacker?
 |  |
| *(for financial institutions)*1. Is the incident determined to have materially affected, or is reasonably likely to materially affect, the viability of operations, the ability to deliver banking products and services, or the stability of the financial sector? Note: if yes, this will trigger the 36-hour notification rule.
 |  |
| 1. Threat level category
 |  |
| 1. Catalyst
 |  |
| **Investigation** |
| 1. Interview the affected users
 |  |
| 1. Determine what internal systems are affected
 |  |
| 1. Analyze all information
 |  |
| 1. Define plan to contain incident
 |  |
| 1. Follow the money trail and determine if any transaction can be stopped/reversed
 |  |
| **Containment** |
| 1. Disconnect affected systems and devices from the network or contact vendor (do not turn off)
 |  |
| 1. Configure firewall to be more restrictive
 |  |
| 1. Change any system password that could have been compromised
 |  |
| 1. Reverse all suspected fraudulent transactions and notify any other organizations (e.g., receiving financial institutions) involved in transactions
 |  |
| 1. Close relevant online accounts if affected
 |  |
| **Analysis** |
| 1. Review affected systems to determine if data was accessed, leaked, deleted, or manipulated
 |  |
| 1. Contact IT forensic firm to determine exact problem
 |  |
| **Recovery** |
| 1. Implement new systems or bring old systems back online
 |  |
| 1. Determine how much money the Organization will return, if applicable
 |  |
| **Notification** |
| 1. Employees
 |  |
| 1. Constituents
 |  |
| 1. Vendors
 |  |
| 1. Partners
 |  |
| 1. Public (media)
 |  |
| 1. Insurance
 |  |
| 1. Local police
 |  |
| 1. FBI Field Office
 |  |
| 1. Internet Crime Complaint Center
 |  |
| 1. U.S. Secret Service
 |  |
| 1. Electronic Crimes Task Force
 |  |
| 1. U.S. Secret Service Field Office
 |  |
| 1. Federal Reserve Bank
 |  |
| 1. Federal regulator
 |  |
| 1. State regulator
 |  |
| 1. FinCEN Suspicious Activity Report (SAR) filed
 |  |
| **Closure** |
| 1. Date/time of final IRT meeting
 |  |
| 1. Final IRT meeting notes
 |  |
| 1. Incident damage
 |  |
| 1. Financial loss
 |  |
| 1. Forensic evidence retention timeframe established
 |  |
| 1. Lessons learned
 |  |
| 1. Forensic evidence retained
 |  |
| 1. Lawyer retained/legal action pursued
 |  |
| 1. Changes to Incident Response Plan
 |  |
| 1. Incident Summary Form submitted to <*insert applicable oversight body, such as IT Committee, Board, etc.*>
 |  |