# Cybersecurity Policy

## Supporting Policy for Information Security Program | Date: 6-30-20

Delete This Image and Insert Your Logo Here

ThreatAdvice

# Cybersecurity Policy

## Contents

# Cybersecurity Policy

# Cybersecurity Policy

## Cyber Security Policy

Creation Date:
Effective Date:
Review Frequency: Annually
Last Review Date:
Board Approval Date:

Control Function: Information Security
Reviewers: Board, CISO, Information Technology & Security Committee
Audience: Internal Audit, Regulatory Examiners, External Audit, All Employees responsible for activities within the cyber security control processes

## Overview

Heightened risk from cyber security threats, such as increased geo-political tensions and threats of aggression, may result in cyber-attacks against U.S. targets and interests. In recent years, disruptive and destructive attacks against financial institutions have increased in frequency and severity. Cyber actors often use malware to exploit weaknesses in a financial institution's computers or networks. They often obtain access to financial institution systems and networks by compromising user credentials and introducing malware through social engineering financial institution employees and contractors with phishing or spear phishing attacks. Another method of attack is to introduce infected external devices to computers and networks through removable media.

Sound cybersecurity risk management principles elaborate on information security standards articulated in the Interagency Guidelines Establishing Information Security Standards as well as resources provided by the Federal Financial Institutions Examination Council (FFIEC) members, such as the FFIEC Statement on Destructive Malware, FIL-3-2020 -Joint Statement on Heightened Cybersecurity Risk January 16, 2020.

When financial institutions apply these principles and risk mitigation techniques, they reduce the risk of a cyber attack's success and minimize the negative impacts of a disruptive and destructive cyber-attack.

While preventive controls are important, financial institution management should be prepared for a worst-case scenario and maintain sufficient business continuity planning processes for the rapid recovery, resumption, and maintenance of the institution's operations. Implementing and maintaining effective cybersecurity controls is critical to protecting financial institutions from malicious activity, especially in periods of heightened risk. Sound risk management for cybersecurity includes the following:

- Response and resilience capabilities: Review, update, and test incident and breach response and business continuity plans.
- Authentication: Protect against unauthorized access. Multifactored authentication for remote access. Includes robust password policies and privileged user monitoring

- Secure System configuration: Securely configure and harden systems and services prior to deployment.
- On-going managed patch management
- Virus and Malware protection programs.
- Secure logging and log aggregation

## Purpose

This Cyber Security Policy is a formal set of rules that comprise a Cyber Security framework by which those people who are given access to or manage company technology and information assets must abide.

The Cyber Security Policy serves several purposes. The main purpose is to inform users: employees, contractors and other authorized users of their requirements for protecting the technology, customer information and information assets of the company. The Cyber Security Policy describes the processes, procedures, controls and plans that we must utilize to identify and protect many of the Cyber threats to those information technology assets.

The Cyber Security Policy also describes the user's and management responsibilities that may be defined in supporting policies such as:

- What is considered acceptable use? (Internet, Email, Software, and Systems Acceptable Use Policies)
- What are the rules regarding Internet access? (Access Policy)

The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains references to policies, procedures, and plans for identifying, detecting and responding to incidents that threaten the security of our technology systems, customer information, and network.

## Scope

This policy applies to the entire organization, including the CEO, President, Senior Management, employees, temporary employees, interns, contractors, and sub-contractors supporting any user, process or application that interfaces in any way with our network, servers, or other information system devices who have access to our information technology assets. Assets include but not limited to, workstations, servers, infrastructure devices such as routers and firewalls, smart phones, operating system software, application software, data, or emails owned, leased, or utilized in providing services to our customers or other internal processes.

## Policy Statement(s)

Basic Cyber Security policy requires adoption of a basic Cyber Security framework where areas important to cyber security can be addressed. The framework must identify, detect, prevent and allows

responses and recovery from cyber-attacks. This must be incorporate conceptions and recommendation from guidance concerning heightened cyber security risks contained in FIL 3-2020 released January 16, 2020, the FFIEC Information Security Examination Handbook and the latest FFIEC Cyber Security Assessment Tool released in 2017.

## FIL 2020 Requirements

This guidance requires use to implement and maintain effective Cyber Security controls which is critical to protecting the institution from malicious activity, especially in periods of heightened risk. Sound risk management for Cyber Security includes the following:

- Response and resilience capabilities: Review, update, and test incident response and business continuity plans.
- Authentication: Protect against unauthorized access.
- System configuration: Securely configure systems and services.

## FFIEC Cyber Security Assessment Tool (CAT)

### Inherent Risk Profile

At least annually review and develop current Inherent Risk Profile according to FFIEC Cyber Security Assessment Tool (CAT) requirements.

### Maturity Assessments

At least annually conduct and review a current Cyber Security maturity assessment according to Cat requirements.

### Cyber Security Risk Appetite Statement

Develop and maintain a Board approved Cyber Security Risk Appetite Statement.

### Board Reporting – Maturity Analysis and Inherent Risk Profile

At least annually review current inherent risk profile and maturity assessment and set objectives for improvement in coming year.

## Key Cyber Security Risk Management Control Areas

Given the heightened threat environment, senior management should reevaluate the adequacy of information technology safeguards against threats, especially safeguards against ransom and other destructive malware. The growing number of attacks highlights the critical importance of making Cyber Security preparedness and resiliency a top priority. Implementing and maintaining effective Cyber Security controls, including threat monitoring, are critical to protecting financial institutions from malicious activity. Key controls that will be implemented and maintained include the following:

### Personnel Security and Cyber Security Training

Establish policies and procedures associated with pre-employment background screening that comply with state and federal regulations and legal requirements. In addition, conduct at time of hire and at least annually security awareness and training appropriate for positions held that contains Cyber Security related training materials and subject matter to include but not limited to Phishing, Spear Phishing, Ransomware, DDOS attacks, DOS attacks, Password requirements, Social Engineering, Email security, and Incident Reporting and Response requirements.

manage the incident response process. Develop incident and breach response procedures/plans and identify relevant stakeholders (both internal and external). Conduct periodic cyber recovery exercises or plan testing to demonstrate that recovery capabilities function as expected. Integrate the cyber security response plan with the overall business continuity management (BCM) program.
Use of cyber insurance as a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure as appropriate and cost effective.

### Cryptographic Management & Encryption

We will define and maintain requirements for encrypting data at rest, data in transit and data in use, commensurate with the information classification of the information requiring protection. Maintain a process for protecting cryptographic keys to preserve the integrity of cryptographic controls. Use of encryption controls shall be determined as a result of a risk assessment and documented in encryption policies.

### Electronic Banking Security (Internet Banking)

Establish policies and standards for web-based services products include mobile banking, cash management, Internet Banking and implement robust multi-factored authentication and multi-layered security as required by regulatory guidance.

### Secure System and Software Life Cycle Management

Perform information security reviews throughout all phases of the system and software management lifecycle to ensure risks are properly identified, addressed and mitigated in a timely and cost-efficient manner. Configure systems using security hardening standards and review configurations periodically to eliminate known cyber security risks. Maintain patch management policy and program for all systems, workstations and other devices that ensures adequate patching to prevent cyber security incidents.

### Wholesale and Retail Banking Security

Establish, maintain and test policies related to ACH, Wires, ACH origination, Swift, CHIPs and other payment related activities especially those conducted utilizing the Internet or are connected to the Internet which are considered high risk from Cyber-attacks.

### Third-party Information Security Risk Management

Establish a process to perform initial and ongoing due diligence of third parties that enter formal business arrangements with us. Emphasis will be on reviewing the vendors Cyber Security controls and practices. Contractual agreements between third parties and must address baseline information security clauses, including, but not limited to, the right to audit and adhere to GLBA data protection requirements, and cyber security incident and breach clauses.

### Cyber Security Control -Logging and Event Monitoring

Develop and implement a process to monitor and review activity associated with information systems. Emphasis on being able to reconstruct and identify activities associated with Cyber Security related events. We must comply with all relevant legal, regulatory and contractual requirements applicable to logging and event monitoring and auditing. Review these logs for anomalous activity utilizing event management tools. These reviews should occur regularly and be performed by qualified personnel.

### Cyber Security Tools and Monitoring

Employ qualified Cyber Security staff in house, or a qualified managed security service to actively monitor systems and the network for cyber threats and vulnerabilities utilizing industry sources such as Financial Services Information Sharing and Analysis Center (FS-ISAC)

### Cyber Security Protection Control – Identity and Access Management

A fundamental component of the Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental

meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources.

Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

Access shall be managed throughout the account lifecycle from the initial identification of a user to the granting, modifying and revoking of user access privileges to confirm that information assets are protected from unauthorized access. Accounts shall be provisioned using the least privilege access principle. Access privileges shall be monitored and reviewed periodically commensurate with their risk classification. Privileged access such as administrators shall be reviewed regularly as those accounts will be the targets of most Cyber-attacks. Passwords must meet the complexity requirements and changed on a regular basis as dictated by the Password Management policy.

## Roles and Responsibilities

### Internal Audit

- Responsible for ensuring vulnerability scans and penetrations tests are conducted according to the annual schedule, reviewed and mitigated according to vulnerability and penetration test procedures and within approved mitigation time periods.
- Responsible for reviewing access, remote access, and privileged access on a regular basis as required by annual Information Technology audit plan.
- Responsible for reviewing technology asset inventories and evaluating end-of-life hardware and software management activities for compliance to policy.

### Information Technology and Security Steering Committee

- Responsible for overall Cyber Security policy and response plan development, maintenance, and approval.
- Responsible for periodic risk assessments, Business Impact Analysis (BIA) and plan adjustments.
- Responsible for ensuring periodic cyber security risk assessments are conducted and identified issues are mitigated.
- Responsible for reviewing and submitting budget requests for Cyber Security protection devices and services.

### Network Administration

- Responsible for developing, maintaining and revising system and device hardening procedures prior to deployment for all information technology devices, software, databases, and operating systems.
- Responsible for developing and maintaining patch management procedures and programs for all information technology systems, workstations, and infrastructure devices.
- Responsible for participation in Incident Breach and Response tests as required.

- Responsible for participating in scheduled recovery exercises to validate backup strategies are complete and recovery procedures are documented and work.
- Responsible for monitoring ongoing Cyber Security related events as identified by Intrusion Detection or Prevention systems.
- Responsible for ensuring all access is granted according to access grant policies including remote access, privileged user access, mobile device access.
- Responsible for ensuring all user identification and authentication is conducted according to password policy, user identification policy, logging policy, and multi-factored authentication policy.
- Responsible for ensuring backup policies and strategies are performed as dictated by the backup policy.

### Chief Information Security Officer (CISO)

The Chief Executive Officer has the responsibility for the overall administration of this policy and making recommendations to the information technology and security steering committee on potential issues with cyber security reliance and posture.

## Related Policy(s)

- Information Security Policy
- System Hardening Policy
- Patch Management Policy
- Security Awareness & Training Policy
- Penetration Test Policy
- Vulnerability Scan Policy
- Privileged User Access Policy
- Data Classification Policy
- Pre-Employment Background Screening Policy
- Acceptable Use Policies (Email, Internet, Systems, Mobile Device, and Software)
- Endpoint Protection Policy

## Definitions

**Acceptable use policy**
A document that establishes an agreement between users and the enterprise and defines for all parties the ranges of use that are approved before users can gain access to a network, email, software, system, mobile device or the Internet.
**Annual Incident Response Testing**
At least once every year, the Information Security Department must utilize simulated incidents to mobilize and test the incident response and recovery plan.
**Cyber-attack**
An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an institution for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; destroying the integrity of the data; or stealing controlled information.
**Cyber event**

# Cybersecurity Policy

A cybersecurity change or occurrence that may have an impact on organizational operations (including mission, capabilities, or reputation).

**Cyber incident**

Actions taken against computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

***Cyber resilience***

The ability of a system or domain to withstand cyber-attacks or failures and, in such events, to reestablish itself quickly.

**Cyber threat**

An internal or external circumstance, event, action, occurrence, or person with the potential to exploit technology-based vulnerabilities and to adversely affect (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

**Cyber security**

The process of protecting consumer and bank information by preventing, detecting, and responding to attacks.

**Data classification program**

A program that categorizes data to convey required safeguards for information confidentiality, integrity, and availability, and establishes required controls based on value and level of sensitivity. Data or Information Classification is applied as outlined in the data classification policy. Customer Confidential Information being the highest data classification level.

**Gramm-Leach-Bliley Act**

The act, also known as the Financial Services Modernization Act of 1999 (Pub. L. 106-102, 113 Stat. 1338, enacted November 12, 1999), required the federal banking agencies to establish information security standards for financial institutions.

**Hardening**

The process of securing a computer's administrative functions or inactivating those features not needed for the computer's intended business purpose.

**Intrusion detection**

Techniques that attempt to detect unauthorized entry or access into a computer or network by observation of actions, security logs, or audit data; detection of break-ins or attempts, either manually or via software expert systems that operate on logs or other information available on the network.

**Intrusion detection system (IDS):**

Software or hardware product that detects and logs inappropriate, incorrect, or anomalous activity. It gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations). IDS are typically characterized based on the source of the data they monitor host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

**Intrusion prevention system (IPS):**

A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target.

**Multi-factor authentication**

The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric).

**Non-public personal information**

# Cybersecurity Policy

For purposes of the Information Security Standards, nonpublic personal information means (i) "personally identifiable financial information"; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any "personally identifiable financial information" that is not publicly available.

**Patch**
Software code that replaces or updates other code. Patches frequently are used to correct security flaws.

**Penetration test**: The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses before they are discovered and exploited by others.

**Personally identifiable financial information**
For purposes of the Information Security Standards, personally identifiable financial information means information (i) a consumer provides to a financial institution to obtain a financial product or service; (ii) about a consumer resulting from any transaction involving a financial product or service between the financial institution and a consumer; or (iii) that a financial institution otherwise obtains about a consumer in connection with providing a financial product or service, such as account balance information, payment history, overdraft history, and credit or debit card purchase information; or the fact that an individual is one of the financial institution's customers.

**Security breach**
A security event that results in unauthorized access of data, applications, services, networks, or devices by bypassing underlying security mechanisms.

**Security event**
An event that potentially compromises the confidentiality, integrity, availability, or accountability of an information system.

**Security Log**
A record that contains log-in and logout activity and other security-related events and that is used to track security-related information on a computer system.

**Vulnerability**
A hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing.

**Vulnerability assessment**
Systematic examination of systems to identify, quantify, and prioritize the security deficiencies of the systems.

## Exceptions and Exemptions

Exceptions to this policy must be submitted by senior management and approved in writing by the Chief Information Security Officer.

## Enforcement and Non-Compliance

We reserve the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. Employees and contracted staff who breach this policy maybe subject to disciplinary action including termination of employment.

# Cybersecurity Policy

## Revision History:

| | Change | Revision | Signature or Authorizer |
|---|---|---|---|
| | New or Replaced Policy | 1.0 | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

ThreatAdvice

# Cybersecurity Policy

## Compliance References

### FFIEC Information Security Examination Handbook

#### II. Information Security Program Management

A comprehensive information security program should incorporate cybersecurity elements, and management should identify, measure, mitigate, monitor, and report cybersecurity-related risks in accordance with the information security program and the ITRM process.

#### II.A.3(a) Supervision of Cybersecurity Risk

Cybersecurity is the process of protecting consumer and bank information by preventing, detecting, and responding to attacks. As part of cybersecurity, institutions should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks. In light of the increasing volume and sophistication of cybersecurity threats, examiners should focus on cybersecurity preparedness in assessing the effectiveness of an institution's overall information security program.

#### II.A.3(b) Resources for Cybersecurity Preparedness

The FFIEC members issued a voluntary Cybersecurity Assessment Tool to help institution boards and management identify risks to their institutions and evaluate their institution's cybersecurity preparedness. In addition, there are other resources available to help management develop and evaluate information security and cyber resilience, such as the NIST Cybersecurity Framework, common approaches developed by the Mitre Corporation, and the U.S. Computer Emergency Readiness Team's (US-CERT) National Cyber Awareness System. Institution management can select a single framework or use a combination of resources to help identify its risks and determine its cybersecurity preparedness. Regardless of the source, frameworks can help management identify a cybersecurity and resilience posture that is commensurate with the institution's risk and complexity.

### Interagency Guidelines Establishing Information Security Standards

### 12 CFR 364, appendix B (FDIC) and 12 CFR 30, appendix B (OCC)

### NIST Framework for Improving Critical Infrastructure Cybersecurity

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical

# Cybersecurity Policy

functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications