Contents

[Banking Regulation, Compliance and Business Standards 2](#_Toc146302473)

[GFH Bank follows NIST 800-53 Rev 5 Cybersecurity Framework consists of five principles: 3](#_Toc146302474)

[System Features Based Upon User Requirements 3](#_Toc146302475)

[Example of Data Security Controls GFH Implements in Protecting Consumer Data: 4](#_Toc146302476)

[References: 4](#_Toc146302477)

## Banking Regulation, Compliance and Business Standards

GFH follows best industries and standards for banking regulations, compliance and standards. GFH have implemented the following guidance, which drives industries best practices into our strategic business model. The following guidance and memorandums govern GFH Bank:

* **Americans with Disabilities Act**
* **Bank Secrecy Act**
* **Bank Service Company Act**
* **Community Reinvestment Act**
* **Consumer Financial Protection Act**
* **Coronavirus Aid, Relief and Economic Security Act (CARES-ACT)**
* **Credit Card Accountability Responsibility and Disclosure Act**
* **Dodd-Frank Wall Street Reform and Consumer Protection Act**
* **Economic Growth, Regulatory Relief and Consumer Protection Act**
* **Electronic Fund Transfer Act**
* **Equal Credit Opportunity Act**
* **Expedited Funds Availability Act**
* **Fair and Accurate Credit Transactions Act**
* **Fair Debt Collection Practices Act**
* **Fair Housing Act**
* **Federal Reserve Act**
* **Flood Disaster Protection Act (FDPA)**
* **Foreign Corrupt Practice Act**
* **Garnishment Rule**
* **General Data Protection Regulation (GDPR)**
* **Gramm Leach Bliley Act**
* **Home Mortgage-Disclosure Act**
* **Home Owners Loan Act**
* **Military Lending Act**
* **NIST Security Control Policies**
* **Payment Card Industry (PCI) Data Security Standards (DSS)**
* **Real Estate Settlement Procedures Act**
* **Risk Management Framework (RMF)**
* **Right to Financial Privacy Act**
* **Sarbanes-Oxley (SOX) act of 2002. Protecting investors from financial scams**
* **Service members Civil Relief Act**
* **Telephone Consumer Protection Act**
* **Truth in Savings Act**
* **Unlawful Internet Gambling Enforcement Act**

## GFH Bank follows NIST 800-53 Rev 5 Cybersecurity Framework consists of five principles:

**Identify:** System assets such as hardware and software, understanding and adhering to cybersecurity polices at both the federal, state and local levels

**Protect**: Protecting and safeguarding assets within the business organization

**Detect:** continuous monitoring of your network in Identifying and taking the necessary steps to mitigate anomalies in the system environment

**Respond:** Notification of security breaches, informing customers of data leakage maintain business operations, update cyber security policies on a semi-annual basis, understanding and knowing risk management

**Recover:** Continuous Continuity of Operations from a cybersecurity incident

The National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, Rev 5 Control Mappings to ISO/IEC 27001 (July 2023): Purpose to implement, operate, monitor, review, maintain and improve information security management systems (ISMS) within the context of risks.

## System Features Based Upon User Requirements

* Intrusion Detection System (IDS)
* Wireless Intrusion Detection System (WIDS)
* Host Base Security System (HBSS)
* Anti-virus software (McAfee)
* Patching (based upon quarterly cycle)
* Multi- factor authentications
* Firewall, routers, switches, SSL encryption
* Authentication timeout notifications

## Example of Data Security Controls GFH Implements in Protecting Consumer Data:

Protections against data leaks: AC-4, AC-5, AC-5, AU-13, PE-19, PS-6, SC-7, SI-4

Asset Management: AC-4, CA-3, CA-9, PL-8, SA-17

Integrity checks mechanisms used to verify software, firmware, and information integrity: SI-7. SI-10

Monitoring for unauthorized personnel, connections, devices, and software is performed: AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4

Incident Response: Recovery processes and procedures are in place to ensure restoration of systems or assets affected by cybersecurity incidents: CP-10, IR-4, and IR-8

**\*Please note: This is not complete list of the security controls. All security controls can be tailored based upon the business environment. Please reference your organizations security policy and the NIST family of security controls for further guidance.**

## References:

*Acts & Regulations*. https://www.aba.com/banking-topics/compliance/acts. Accessed 22 Sept. 2023.

“Cybersecurity Framework Crosswalk.” *NIST*, Jan. 2020. *www.nist.gov*, https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks/cybersecurity-framework-crosswalk.

Initiative, Joint Task Force Transformation. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication (SP) 800-39, National Institute of Standards and

“Security and Privacy Controls for Information Systems and Organizations.” *Security and Privacy Controls for Information Systems and Organizations*, National Institute of Standards Technology, 8 July 2023, https://crsc.nis.gov/pubs/sp/800/53/r5/upd1/final.

“The Five Functions.” *NIST*, Apr. 2018. *www.nist.gov*, <https://www.nist.gov/cyberframework/online-learning/five-functions>.