SIFMA Data Protection Principles

Financial companies need to collect and share sensitive information to run their everyday business. Members of SIFMA's Data Protection Working Group developed a set of principles for the protection of sensitive data that align to the industry-developed Financial Sector Profile and NIST Cybersecurity Framework. Drawn from financial firm experiences with the protection of sensitive data they hold, these principles also extend to sensitive industry data which is held elsewhere in the industry, such as at third parties, vendors, and regulators and supervisors.

- **Data collection:** Limit the collection of sensitive data to that which is directly relevant and necessary to accomplish a specified purpose
- **Data usage:** Implement preventative and detective controls limiting access to sensitive data to authorized users only
- **Data sharing:** Develop policies to protect information when it needs to be shared with external entities
- **Data Disposal:** Securely eradicate, dispose, or destroy sensitive data when appropriate
- **Overarching Best Practices:** Implement controls and policies to maintain a robust information security environment

Data Collection

1. Limit the collection and disclosure of sensitive financial institution data to that which is directly relevant and necessary to accomplish a specified purpose. *(NIST Cybersecurity Framework, p. 16)*[1]

Data Usage

2. Limit access to sensitive financial institution data to authorized users and review access on a periodic basis and upon change of job function or role. *(PR.AC-1, PR.AC.-2, PR.AC-4)*[1]
3. Use multi-factor authentication to protect against unauthorized access to sensitive financial institution data and for any individual accessing internal networks from an external network. *(PR.AC-1, PR.AC-3, PR.AC-4)*[1]
4. Implement Data Loss Prevention (DLP) controls to ensure that sensitive financial institution data cannot be removed without management authorization. *(DE.CM-7, PR.DS-5, PR.PT-2)*[1]
5. Maintain a detailed audit trail throughout the data lifecycle (receipt/creation, usage, deletion) to ensure the accessibility and location of sensitive financial institution data can be determined at all times. *(ID.AM-1, PR.AC-2, PR.DS-1, PR.DS-2, PR.DS-3, PR.PT-1, PR.PT-2)*[1]

[1] *Originally known as the Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, the Financial Services Profile (FSP) in Europe, and the Profile in the United States, the non-profit Cyber Risk Institute's (CRI) Cybersecurity Profile was a collaborative effort of 150 financial firms and more than 300 bank representatives over several years, with input from multiple regulatory agencies and experts. The result is a unified harmonized approach to cyber security assessments that can be used by the smallest and the largest financial services firms: banks, securities, and insurance. The CRI Cybersecurity Profile is recognized as a global cyber tool and convergence instrument bringing together a catalogue of global security standards, regulations, and legal framework requirements. Ownership and management of the Profile transitioned from FSSCC to the CRI in January 2020.* www.cyberriskinstitute.org

[2] https://www.nist.gov/cyberframework

SIFMA Data Protection Principles

Data Sharing

6. Review the security of an external entity (e.g., subcontractor, other government agency) prior to providing access to sensitive financial institution data and on an ongoing basis. *(ID.RA-3)*[1]
7. Use encryption with strong key management practices and physical protection of sensitive financial institution data in transit, including interagency transfers, and at rest. *(NIST Cybersecurity Framework: PR.AC-2, PR.DS-1, PR.DS-2)*[1]

Data Disposal

8. Securely eradicate, dispose of, or destroy sensitive financial institution data when there is no longer a valid business purpose or to satisfy regulatory or retention requirements and prior to disposal, reuse, or reassignment of electronic media and devices. *(PR.DS-3, PR.IP-6)*[1]

Overarching Data Protection Program Best Practices

9. Implement a vulnerability management program to ensure the timely identification and resolution of any issues, gaps, or weaknesses. *(ID.RA-2, ID.RA-3, PR.IP-12)*[1]
10. Conduct penetration tests (e.g., manual ethical hacking, dynamic analysis) of applications handling sensitive financial institution data at least every 12 months, after significant changes, and prior to production use. *(DE.CM-8)*[1]
11. Perform vulnerability scans on applications with sensitive financial institution data at least quarterly and after significant changes. (DE.CM-8)[1]
12. Provide for timely remediation of security assessment findings associated with the storage, transmission, or processing of sensitive financial institution data. *(RS.MI-3)*[1]
13. Ensure all end users receive periodic security awareness training that includes training on the identification and reporting of a phishing attack and processes to protect sensitive data. *(PR.AT-1, PR.AT-4)*[1]
14. Institute a process to notify the financial institution of an information security violation or potential information security incident that affects financial institution data or services. *(RS.CO-2, RS.CO-3)*[1]
15. Establish a secure process through which the results from security assessments of systems and processes associated with the storage, transmission, or processing of sensitive financial institution data can be provided to affected financial institutions. *(ID.RA-2, ID.RA-3, ID.RA-6, RS.CO-5)*[1]

[1] *Originally known as the Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, the Financial Services Profile (FSP) in Europe, and the Profile in the United States, the non-profit Cyber Risk Institute's (CRI) Cybersecurity Profile was a collaborative effort of 150 financial firms and more than 300 bank representatives over several years, with input from multiple regulatory agencies and experts. The result is a unified harmonized approach to cyber security assessments that can be used by the smallest and the largest financial services firms: banks, securities, and insurance. The CRI Cybersecurity Profile is recognized as a global cyber tool and convergence instrument bringing together a catalogue of global security standards, regulations, and legal framework requirements. Ownership and management of the Profile transitioned from FSSCC to the CRI in January 2020. www.cyberriskinstitute.org*

[2] https://www.nist.gov/cyberframework