Information Security Principles

March 2024

CeriFi is an ally for financial and legal learning. Our products include highly specialized information-enabled software and tools for financial planning, advanced designations, Fintech crimes, tax, accounting and legal.

Our reputation for delivering dependable and credible services is upheld by a robust information security management framework, which is reinforced by an extensive array of security policies, standards, and practices.

This document helps outline CeriFi's approach to information security and risk management.

White Paper

Contents

Information Security Strategy Overview

CeriFi operates a global information security organization that is aligned with the NIST CSF.

CeriFi takes a proactive approach to data security, structuring our cybersecurity program to align with the industry recognized NIST Cybersecurity Framework. By continuously improving our capabilities in threat prevention, detection, and response, we aim to evolve our defenses to match emerging business needs and customer expectations.

Core focuses guide our program: Increasing maturity in cybersecurity capabilities, modernizing our security technology stack to support innovation, and instilling a culture centered on data protection. CeriFi remains dedicated to robust security practices that enable our customers to advance with confidence.

Security Organization

Program and Practices

CeriFi has assembled a dedicated team of security and privacy experts committed to safeguarding our products and services. This includes both internal and external leading trusted industry partners. This cross-functional group oversees our Information Security Footprint, which has earned endorsement from the Executive Committee through its rigorous data protection standards.

By aligning with the industry standard NIST Cybersecurity Framework, our policies, controls, and communication processes enable secure product development as well as robust security environments. From development to deployment, CeriFi focuses at each stage on upholding confidentiality, integrity, and availability of customer data. Our programmatic approach allows us to ingrain proactive security measures throughout our systems and culture. With executive-level oversight, our experts continue driving cyber risk management maturity to match both internal business needs and customer expectations.

Policy and Standards

CeriFi has implemented robust internal policy governance, with our Information Security Risk Management team overseeing core policies and standards aligned to the NIST Cybersecurity Framework. These infosec principles apply across people, processes, and technologies to uphold confidentiality, integrity, and availability of products and services.

We pursue continuous enhancement through regular reviews that adapt policies to address evolving threats, regulatory changes, and customer expectations. With improving defense capabilities via aligned standards, vigilant governance, and enabling infrastructure, CeriFi strives to ingrain proactive measures that match both dynamic business contexts and exacting industry benchmarks.

Our Employees

Code of Conduct

All CeirFi employees are subject to annual Ethics training and are required to acknowledge their consent to abide by its terms on an annual basis. The training sets forth the highest ethical standards of conduct for how we operate in all the countries where we do business. The See Something Say Something mantra– is incorporated into our training and helps serve as a guide for our workforce.

If misconduct is suspected, a report can be made to a supervisor, Human Resources, or our Chief HR Officer without fear of retaliation.

CeriFi will take prompt and appropriate action if it determines that a violation of the Ethics occurs, which may result in disciplinary action, up to and including termination of employment.

The Ethics also incorporates the Information Security Handbook, which describes the policies and guidance that must be followed when handling information or using CeriFi assets or resources.

CeriFi's Code of Business Conduct and Ethics underscore our Trust Principles – integrity, independence, and see something say something.

Background Screening

Conducting background checks is a crucial step in CeriFi's hiring process. Confirming background details helps assess a candidate's general suitability for employment or an employee's fitness for a specific role. CeriFi's background checks, in compliance with legal regulations, may encompass verifying identification, previous employment, criminal records, global security screenings, and educational qualifications, tailored to the country and positions requirements.

Security Training

Every worker, whether an employee or a contractor, who has access to CeriFi's systems and data, must undertake an obligatory Information Security and Privacy course on an annual basis. Additionally, CeriFi's security awareness team regularly carries out company-wide phishing simulation drills for all employees and contractors. These phishing campaigns are crafted by CeriFi to promote secure practices within the organization.

CeriFi offers tailored training to particular employee groups when needed. We collaborate with external vendors to offer customized learning programs for employees of all proficiency levels.

Cyber Risk Management

CeriFi has specialized experts committed to enhancing information security measures. Their goal is to pinpoint potential risks to our information assets and prevent any unauthorized access, loss, or misuse. To effectively manage these risks, we employ a range of controls, security devices, monitoring tools, and threat models to assess our systems and network.

The product and technology teams collaborate with information security experts to perform architecture assessments, security penetration tests, vulnerability scans, application security tests, and technical compliance reviews. These activities aim to pinpoint and address security threats within CeriFi.

Third party PEN tests are conducted periodically throughout the calendar year against various LMS product lines. These third-party Penetration Tests ensure that an impartial, security centric trusted industry leader is conducting the test.

CeriFi has developed a comprehensive enterprise risk management framework that includes quarterly cyber security risk assessments.

Cyber Risk Analytics and Security Ratings

CeriFi is dedicated to aligning with external cyber risk analytics and security ratings criteria, as shown by assessments from third-party scanning partners like DeepSeas. We employ a risk-focused method and a clear procedure to consistently observe and resolve issues highlighted by DeepSeas, in addition to our internal systems and tools.

Data Security

CeriFi implements a Data Loss Prevention (DLP) initiative aimed at reducing the cybersecurity, business, and legal threats linked to both deliberate and accidental data breaches. This program utilizes a range of data loss prevention technologies across various assets and educates employees on appropriate data management practices.

Data Disclosures

CeriFi regards its duties as a data controller and data processor with great importance and has established a procedure to handle requests from individuals seeking to exercise their rights to access, correct, modify, or delete their data.

For further details, please refer to the CeriFi Privacy Policy accessible on the website: https://www.cerifi.com/en/privacy-policy.html.

Data Encryption

At CeriFi, safeguarding our data and that of our clients is a top priority. We adhere to industry standards by implementing data encryption measures. Our encryption protocols aim to maintain the privacy, reliability, and accessibility of data, and to deter any unauthorized viewing, usage, or release. Furthermore, these policies and standards are crafted to secure data whether it's in transit or at rest.

Data Storing and Processing

CeriFi utilizes a number of data centers located around the world to cater to our global operations, in partnership with various cloud service providers. Moreover, we make use of specific regions and hosting sites in certain countries to address latency issues and comply with contractual, legal, and regulatory obligations.

Identity and Access Management

CeriFi tracks all corporate owned devices through various dedicated channel portals.

CeriFi implements identity security measures across the network, infrastructure, product environments, and applications for employees, contractors, and third-party suppliers. The identity and access controls at CeriFi are crafted in alignment with recognized industry standards and best practices. These include principles like least privilege, segregation of duties, unique user IDs, robust password policies, and multi-factor authentication. Furthermore, CeriFi regularly undertakes internal and external assessments to gauge the efficacy of its access controls.

As part of our commitment to maintaining the highest levels of security for our systems, we take great care in managing administrator access. This involves implementing a range of measures to ensure that only authorized personnel are able to access sensitive areas of our systems. One key aspect of this is the use of multi-factor authentication, which requires users to provide multiple forms of identification before they can gain access. This might include a password, an authentication app, a biometrics scan, or a security token. By enforcing the use of multi-factor authentication, we are able to significantly reduce the risk of unauthorized access and protect our systems from potential security breaches.

An Enterprise Grade Password Manager is a sophisticated tool that is employed to ensure that passwords are managed and secured with the utmost care. This type of password manager is designed to meet the needs of large organizations, where the management of passwords can be a complex and time-consuming task. With an Enterprise Grade Password Manager, passwords are stored securely and encrypted, ensuring that they cannot be accessed by unauthorized individuals. This tool also provides features such as password generation, password sharing, and password expiration, which help to ensure that passwords are strong, unique, and regularly updated. By implementing an Enterprise Grade Password Manager, CeriFi introduces an additional layer of confidence that our passwords are being managed in a way that meets the highest standards of security and compliance.

Media Disposal

CeriFi meticulously tracks the status of all corporate equipment such as laptops, tablets and smartphones with various Device Management Systems as well as hardware tracking portals. When a system is retired, authorized individuals verify that the system is formatted and all corporate data purged. Physical destruction when necessary is conducted by a certified partner organization.

Contractor Cyber Risk Management

The CeriFi Contractor Cyber Risk Management Program involves conducting due diligence to confirm that contractors, vendors and partners have the necessary controls in place to safeguard our data and that of our customers. Third-party vendors must adhere to CeriFi's standards and controls for data processors as stipulated in their contracts, which cover security and privacy requirements. Assurance evaluations are carried out on vendors and third parties to ensure they are meeting the obligations outlined in their contracts.

Cloud Security

CeriFi’s cloud deployments leverage security inherent to leading third-party cloud providers by utilizing native security services. Additionally, CeriFi increases cloud defense in the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) environments by employing threat detection capabilities via various tools.

CeriFi makes use of the security features offered by top third-party cloud providers to enhance security in cloud deployments through the utilization of their native security services.

To ensure consistency and compliance with CeriFi's security policies and standards, cloud service provider account setup and maintenance follow structured processes throughout the development lifecycle. Cloud applications must undergo a thorough security assessment before being launched into production to verify security requirements and guarantee the presence of necessary controls for safeguarding cloud resources.

CeriFi utilizes top industry tools to scan public cloud environments. It includes controls that guarantee the cloud setup aligns with CeriFi's policies and security architecture guidelines. This significantly boosts CeriFi's capacity to uphold proper cloud configuration protocols in our public cloud infrastructure.

CeriFi utilizes Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Managed Services from leading public cloud providers in the industry. This involves CeriFi working with these providers under a shared responsibility model to safeguard customer data. CeriFi conducts annual assessments of the security features of these cloud service providers to verify that they align with our security standards.

Product Security

CeriFi follows industry standard security practices throughout the Software Development Life Cycle. The product development process includes collaboration with critical infrastructure and architecture experts to ensure the implementation of security best practices from initial discovery to release of applications and services. To ensure standards are met and exceeded, every code change is meticulously reviewed and subsequently scanned using automated processes for potential issues. Also, quarterly vulnerability scans and penetration tests are conducted by external teams. Issues uncovered by these processes are afforded top priority in development backlogs.

Network and Infrastructure Security

At CeriFi, we implement a combination of detective and preventative security measures throughout our network to establish a multi-layered defense system against contemporary threats.

CeriFi takes the security very seriously and employs a comprehensive approach to protect against modern threats. Our strategy involves both detective and preventative defensive security controls that work together to achieve defense-in-depth.

CeriFi has implemented various technologies at critical points within the distributed network environment to ensure a multi-levelled layered approach to securing our environments. This includes segregation of the production environment and accounts from operational systems and accounts. This nuanced security approach helps to ensure segmentation and isolation of production and operational assets to further eliminate the potential for lateral movement from potential bad actors.

By using these measures, we can ensure that our network is secure from potential attacks and that any threats are detected and dealt with quickly and effectively. Our goal is to provide a safe and secure environment for our clients to conduct their business with peace of mind.

We ensure that our infrastructure is protected by implementing robust and secure configurations that are based on industry best practices for configuration management. Our approach includes the use of various technologies such as mobile device management, antivirus, endpoint detection and response, least privilege functionality, vulnerability scanning, phishing defense, and encryption. By utilizing these tools, we are able to provide a secure compute environment for our users to work in and ensure that our products are hosted in a safe and secure manner. Our commitment to security is paramount, and we continuously monitor and update our systems to stay ahead of any potential threats.

Mobile Device Security

At CeriFi, we put in place a Mobile Device Management (MDM) Policy to ensure the safe use of mobile devices such as smartphones and laptops. This policy outlines strict security guidelines and criteria that must be followed by all employees who use these devices. One of the key policy procedures is the use of AutoPilot MDM enrollment for all CeriFi laptops to ensure proper authorized devices can connect to the company's infrastructure. Another important aspect of CeriFi's MDM Policy is the ability to remotely delete company data if necessary. This feature provides an added layer of security in case a device is lost, stolen or otherwise compromised.

In addition to these measures, CeriFi also administers company cellphones via a centrally managed MDM. This ensures that all devices used for work purposes meet the same security standards and are protected from potential threats. Overall, CeriFi's MDM Policy is an essential tool for maintaining a secure work environment and protecting sensitive information from unauthorized access.

Security Defense and Response

CeriFi employs multiple automated real time detection and response systems to help ensure 24x7x365 security analysis and alerting.

Logging and Monitoring

CeriFi employs automated logging to effectively monitor and manage various technology assets in our environment. This advanced system enables us to provide real-time alerting, ensuring that we are always working towards staying one step ahead of potential threats.

By closely monitoring key and strategic platforms within the organization, we are able to add an extra layer of defense against malicious behaviors and target key indicator sets to better defend critical platforms and services. This elevated level of monitoring helps to ensure the security and integrity of CeriFi's technology assets, providing peace of mind for both the company and its clients.

Security Operations

CeriFi has deployed a range of advanced security measures across our data assets and cloud footprint to detect, disrupt, and prevent malicious activities such as spoofing, hijacking, malware, and ransomware. Our proactive security monitoring tools operate on multiple layers, providing round-the-clock protection for our operations. Our dedicated team of security experts continuously monitor and analyze data, networks, services, and systems to identify and deflect potential security threats, ensuring the highest level of protection for our organization.

Security Incident Management

At CeriFi Incidents are carefully evaluated and prioritized based on their level of criticality, and are then assigned to dedicated incident leads. We follow a set of documented response practices, as well as established communication and escalation protocols. To ensure that all incidents are handled with the utmost care and attention, we coordinate our efforts across multiple CeriFi functions. In the event that an incident requires further attention, we have pre-determined escalation procedures in place that include notification protocols for our Senior Management Team.

At CeriFi we utilize a combination of third-party open-source tools, commercial off-the-shelf tools, and proprietary in-house tools and scripts for both remote and on-site investigations. Our team follows industry best practices, including chain of custody and evidence handling procedures, particularly for sensitive investigations such as privacy incidents.

Vulnerability Management

At CeriFi, we employ a comprehensive approach to investigations, utilizing a blend of third-party open-source tools, commercial off-the-shelf tools, and proprietary in-house tools and scripts for both remote and on-site inquiries. Our team adheres to industry-leading protocols, including chain of custody and evidence handling procedures, especially for delicate investigations such as privacy incidents.

Patch Management

CeriFi's patch management standard is aligned with the industry's best practices and adheres to product security principles that meet specific requirements. Our approach guarantees that patches are communicated, rated, and deployed efficiently. Our standard mandates that technology teams prioritize security patches based on their significance and deploy them within specific time frames. To mitigate unknown threats, we also employ forced patching protocols. Furthermore, we may implement additional Endpoint Protection security controls to mitigate known threats, as needed. We monitor both OS and third-party applications and deploy security patches on a regularly maintained sequence.

Endpoint Protection

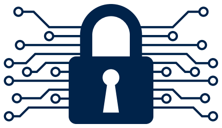
CeriFi, ensuring the security of our networks and customers is our top priority, and we treat malware threats with utmost seriousness. To protect their well-being, we have put in place a thorough endpoint protection plan that incorporates antivirus scanners to block the transmission of harmful content.

Our strategy combines endpoint and antivirus solutions that cater to both systems and email settings, allowing us to identify and block malicious content before it reaches CeriFi. The virus signature files are regularly updated automatically, and our system administrators are quick to install important antivirus software updates as soon as they are released.

Cyber Intelligence

At CeriFi, we employ a diverse range of commercial and open-source intelligence sources to continuously monitor, analyze, and mitigate potential cyber threats to our organization. Our intelligence includes indicators of compromise, attacker tactics and techniques, and evolving motivations and targeting across threat groups. As we identify new threat details, we promptly update our network and endpoint detection and prevention technologies to better defend against these emerging threats.

Furthermore, we actively participate in strategic threat sharing forums and partnerships, which provide us with increased visibility into the latest threat trends observed across industries aligned with CeriFi.



Effective patch management, robust endpoint protection, and multi-layered, sophisticated enterprise-grade cyber intelligence are essential components of the comprehensive CeriFi CyberSecurity infrastructure.

Asset Management

At CeriFi, safeguarding our information technology assets and data is of utmost importance. To achieve this, we have implemented and maintained a comprehensive set of asset management practices and technologies across our enterprise. These include asset identification and classification, infrastructure management, acceptable use policies, and proper asset decommission and disposal procedures. We are committed to protecting our assets and data, and we continuously strive to improve our practices to ensure the highest level of security.

Assets included in the inventory are allocated to an owner who is responsible for preserving the asset's characteristics. This entails the owner being answerable for monitoring the asset's state, whereabouts, and other pertinent details. By assigning a specific owner to each asset, it simplifies the inventory management procedure and guarantees that each asset is being adequately maintained.

Change Management

CeriFi adheres to the ITIL best practices by implementing a meticulous change control process. This process is specifically designed to ensure that changes are managed using a formal development lifecycle methodology, thereby providing safeguards throughout the technology lifecycle.

This process facilitates advantageous modifications to be implemented with minimal interference to business operations, guaranteeing the highest standards of service quality and availability are upheld.

To ensure the uninterrupted delivery of services, a formal approach is employed to plan, coordinate, schedule, approve, assess risks and potential impacts, and track all changes made to a controlled environment. This safeguards the ability to provide services while implementing changes to software, configuration, and hardware, which may include databases, connectivity, new hardware implementation, and updates to existing hardware.

Contact your CeriFi Representative for more information.

For More Information

□ About our products & Services
https://cerifi.com/

□ View our Privacy Policy:
https://cerifi.com/privacy-policy

□ View our Terms of Service
https://cerifi.com/terms-conditions

□ Contact your CeriFi Representative or contact us online at:
https://cerifi.com/contact-us