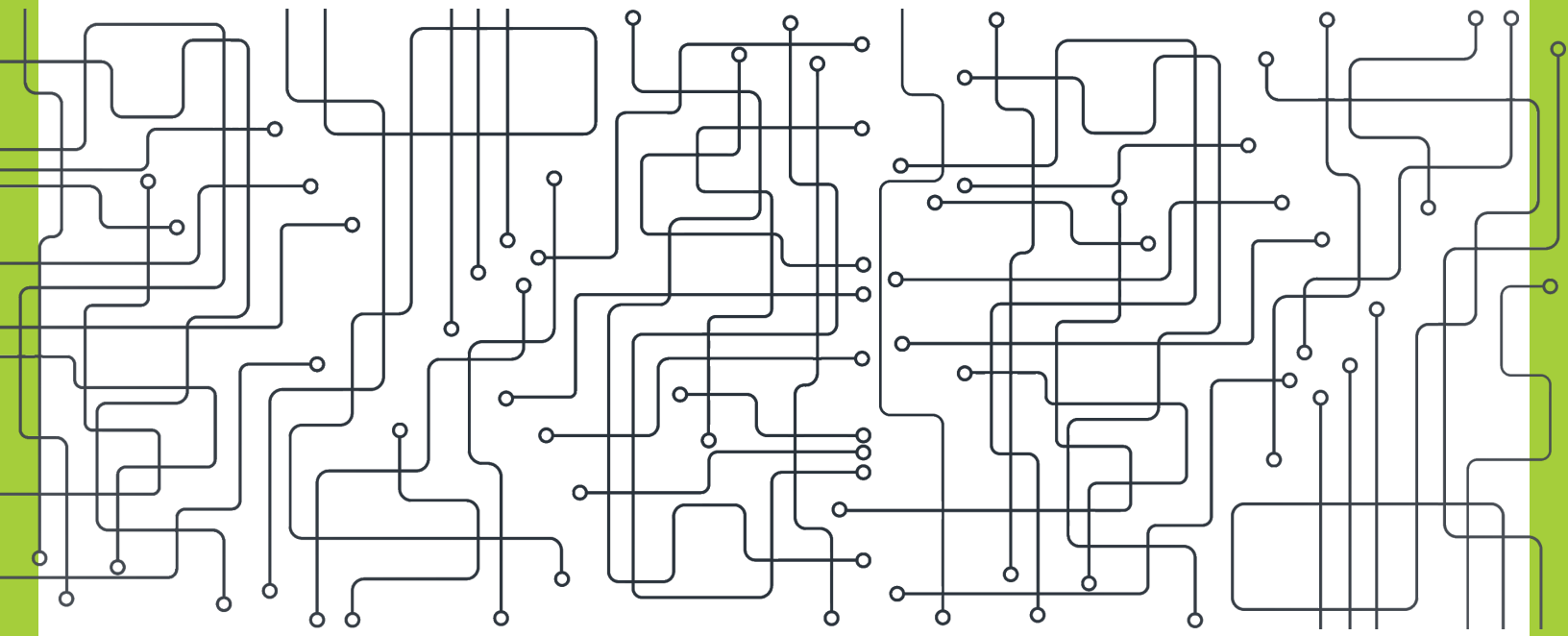
12 Responses: DOL Cybersecurity Best Practices

Sentinel Group takes information security and the safeguarding of participant and plan sponsor information very seriously. This has been a top priority for Sentinel for many years, and we hope you'll rest easy knowing that we'll keep you informed as we continue to safeguard your information and the information of your plan participants.

The following responses have been provided to assist you with meeting your obligations as a plan sponsor – and as a fiduciary. In light of the Department of Labor's (DOL's) guidance on cybersecurity, we recommend you review the data security protocols outlined on the following pages.

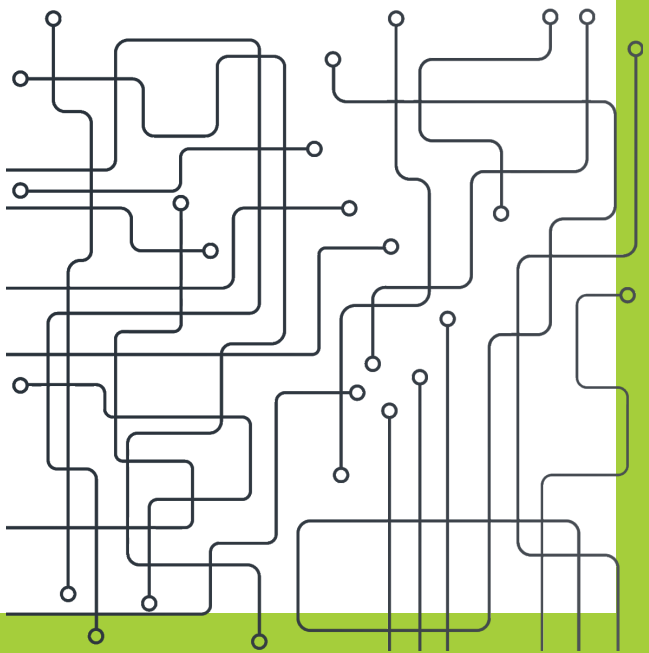


1 Does Sentinel have processes and systems for dealing with cybersecurity threats and protection of personally identifiable information?

Sentinel has a formal cybersecurity program in place that involves a multi-faceted approach to data and computer-environment security. Sentinel follows the NIST framework (**https://www.nist.gov/cybersecurity**) for overall security strategy and operational controls. Like many programs at Sentinel, cybersecurity begins with executive sponsorship and the recognition that the program is a top, firm-wide priority and cybersecurity is every employee's job.

Select elements of Sentinel's Cybersecurity Program include:

- **Threat and Risk Mitigation**
- **Incident Identification, Response and Disaster Recovery**
- **Network and Systems Detection and Alerting**
- **Encryption and Data Privacy**
- **Employee Training and Client Awareness**
- **Formal Testing and Issue Remediation**
- **Secure IT Development and Operational Practices**
- **Vendor Due Diligence**
- **Proactive Network Monitoring**
- **System Access Controls**



2 Does Sentinel conduct periodic assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences?

Sentinel has formal, established processes for assessing risks, which are overseen by Sentinel's Risk Committee that meets regularly to discuss Cyber and Operational risk topics. This team is comprised of various executives including the Chief Information Security Officer, Chief Operating Officer, Chief Compliance Officer and Chief Financial Officer. Any potential risks from across business units are discussed and remediated. Relevant topics are also promoted to the firm's Operating Committee, which is comprised of business leaders across Sentinel's enterprise. Risk awareness and remediation requires constant attention as the business evolves and as threats change.

Annually, Sentinel engages third-party security consultants to perform external penetration testing. Penetration testing is a third-party authorized simulated cyberattack across Sentinel's systems and environments to test security defenses and infrastructure. Issues are communicated to Sentinel's Risk Committee and senior leadership, prioritized, and assigned to the appropriate resources. Remediation plans are documented and overseen by the Chief Information Security Officer.

Aside from identifying opportunities to strengthen Sentinel's infrastructure, this activity also helps better prepare Sentinel as the threat landscape evolves.

3 Does Sentinel maintain independent third-party certifications?

On an annual basis, Sentinel provides several independent third-party certifications.

The SOC 1 Type 2 examination covers our Health, Welfare, and Retirement Plan Services. As part of this scope, controls in areas of administration, operations, information technology and finance are reviewed. The controls addressed in a SOC 1 examination are those that a System and Organization implements to prevent, or detect and correct, errors or omissions in the information it provides to user entities.

The SOC 2 Type 2 examination covers our Health & Welfare and Retirement Plan Services, Financial Planning and Investment Advise Services, Insurance Product Services, and Investment Brokerage Services. Reporting on controls relevant to Security were examined. The scope includes that information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

The examinations were performed by an independent CPA firm, Schellman & Company, LLC for the review period of July 1, 2021 – June 30, 2022.

3 Does Sentinel maintain independent third-party certifications? *Cont'd.*

Service Provider Excellence:
CEFEX®, Centre for Fiduciary Excellence, LLC, has renewed the certification of Sentinel Group, as adhering to the American Society of Pension Professionals & Actuaries (ASPPA) Standard of Practice for Retirement Plan Service Providers

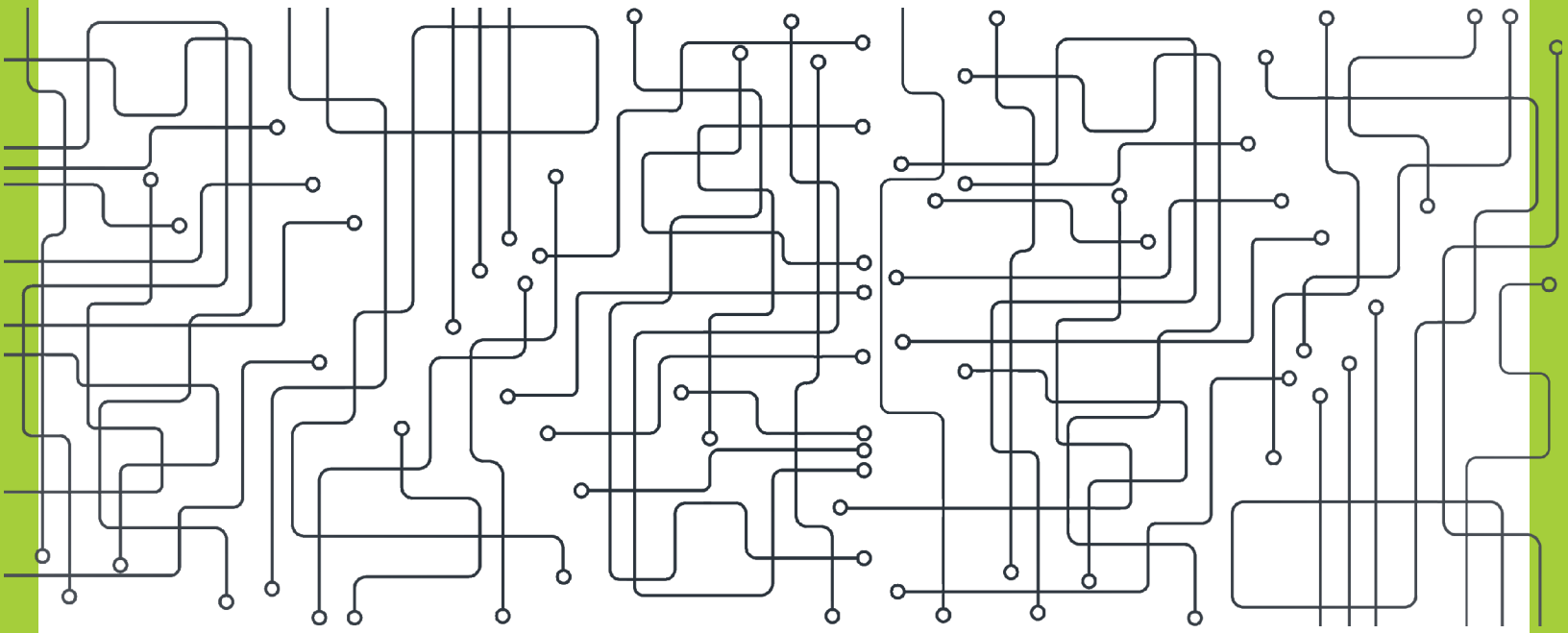
CEFEX® uses 2 classifications: 1. in-house recordkeeping services and 2. administration services (i.e. third party administration). The Standard includes best practices for governance, organization, human resources, operations, planning, systems, and disclosure, as defined by a cross-industry task force established in 2007. Sentinel Group is registered at **http://www.cefex.org/ASPPAAdministration/**.

Fiduciary Excellence:
Sentinel Pension Advisors, Inc. has received renewed certification from CEFEX®, the Centre for Fiduciary Excellence. As a certifying organization, CEFEX provides independent recognition of a firm's conformity to a defined Standard of Practice. It implies that a firm can demonstrate adherence to the industry's best practices, and is positioned to earn the public's trust. This registration serves investors who require assurance that their investments are being managed according to commonly accepted best practices.

4 Does Sentinel have a Chief Information Security Officer or equivalent role?

Sentinel employs a Chief Information Security Officer (CISO). As head of Information Security, this role is responsible for all aspects of Sentinel's enterprise-wide information security, information technology risk management, security preparedness, and systems development.

Sentinel also believes that cybersecurity is not just the job of one person or a department; it is every employee's job to be aware of potential issues and to be on the lookout for potential new ones. Data is the most important asset the firm has, and protecting it is critical to every business unit's success.



5 Does Sentinel have strong access control procedures that are maintained and frequently reviewed?

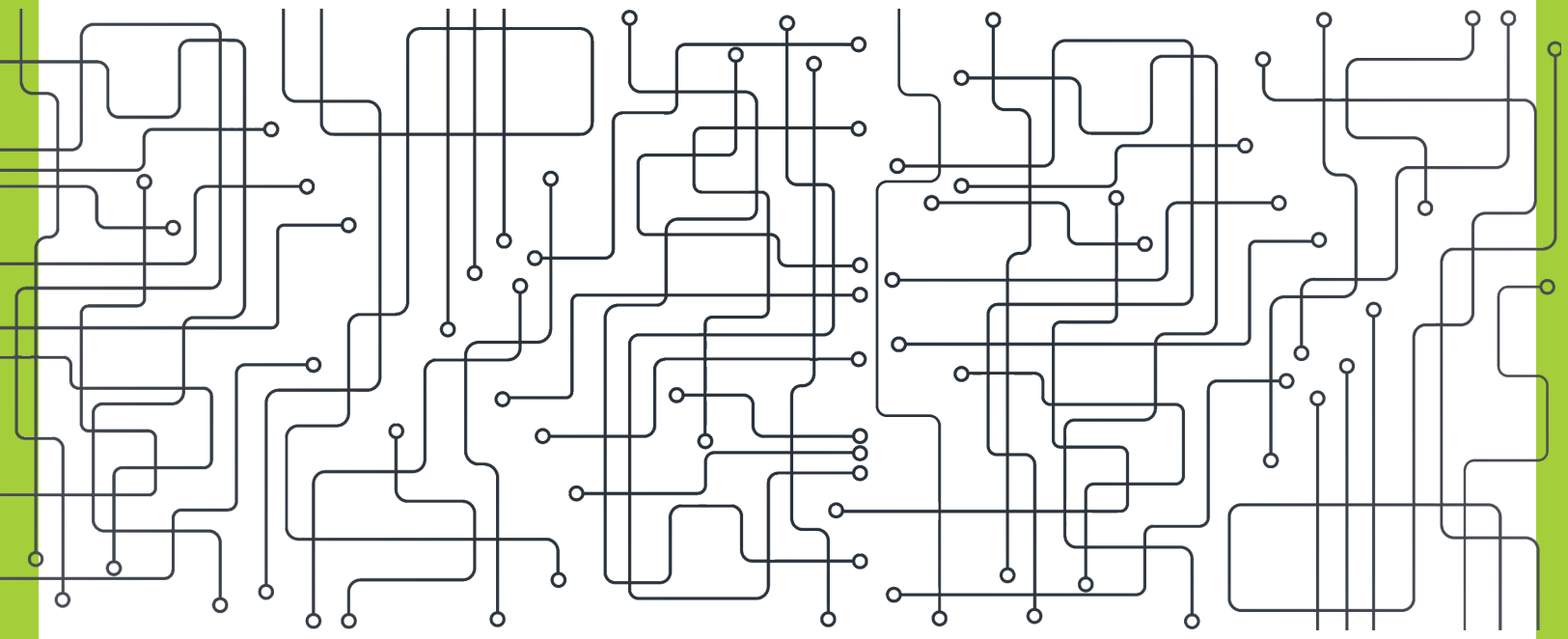
Sentinel ensures systems access and employee roles are controlled and monitored. In addition to having employees sign off on an acceptable use policy, Sentinel maintains that employees have the access they need to perform the responsibilities of their job, but do not extend access beyond that.

Components of Sentinel's access controls include, but are not limited to:

- **All employees use unique, complex passwords to access the Sentinel's environment. These credentials are required to be updated on a frequent basis.**
- **All employees must utilize multi-factor authentication, in addition to unique credentials, to access Sentinel's environment.**
- **Access to systems, data assets and associated facilities are limited to authorized employees based on role and job function.**
- **Access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with Sentinel's access control policy.**
- **Sentinel's Information Technology employs tools to detect, review, and remediate any unauthorized access.**
- **Task-specific controls and procedures are maintained and followed in relation to transactional activities (account setup, participant initiated requests, etc.).**
- **Control procedures are audited annually by an outside third party.**

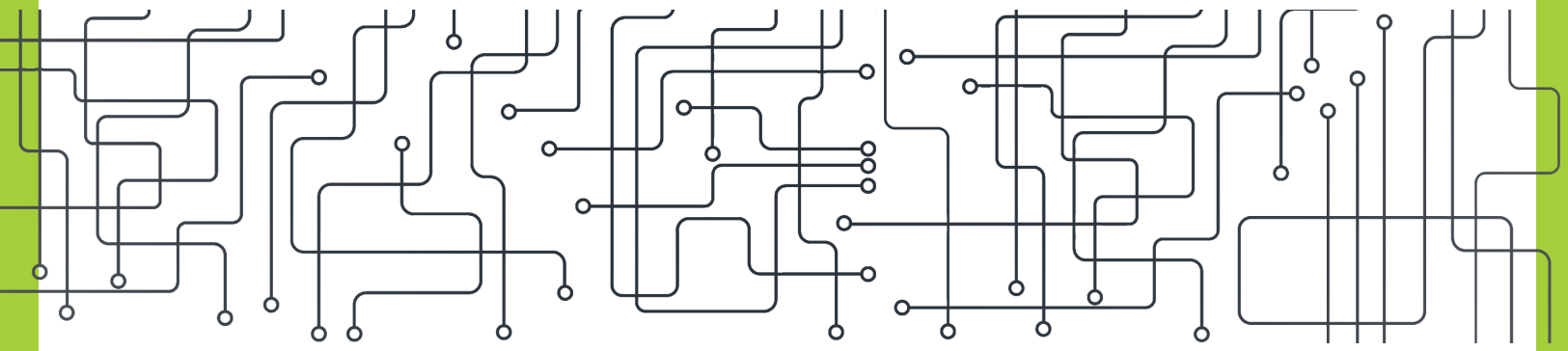
6 Are any/all assets or data stored in a cloud or managed by a third party provider subject to appropriate security reviews and independent security assessments?

As part of Sentinel's internal controls, we frequently review all associated vendors and data handles. Annually, Sentinel conducts a formal review of its vendor list. Vendors are ranked by various risk factors, including the sensitivity of data they have access to. Relevant due diligence is conducted to ensure those partners and vendors meet necessary cybersecurity and data security standards.



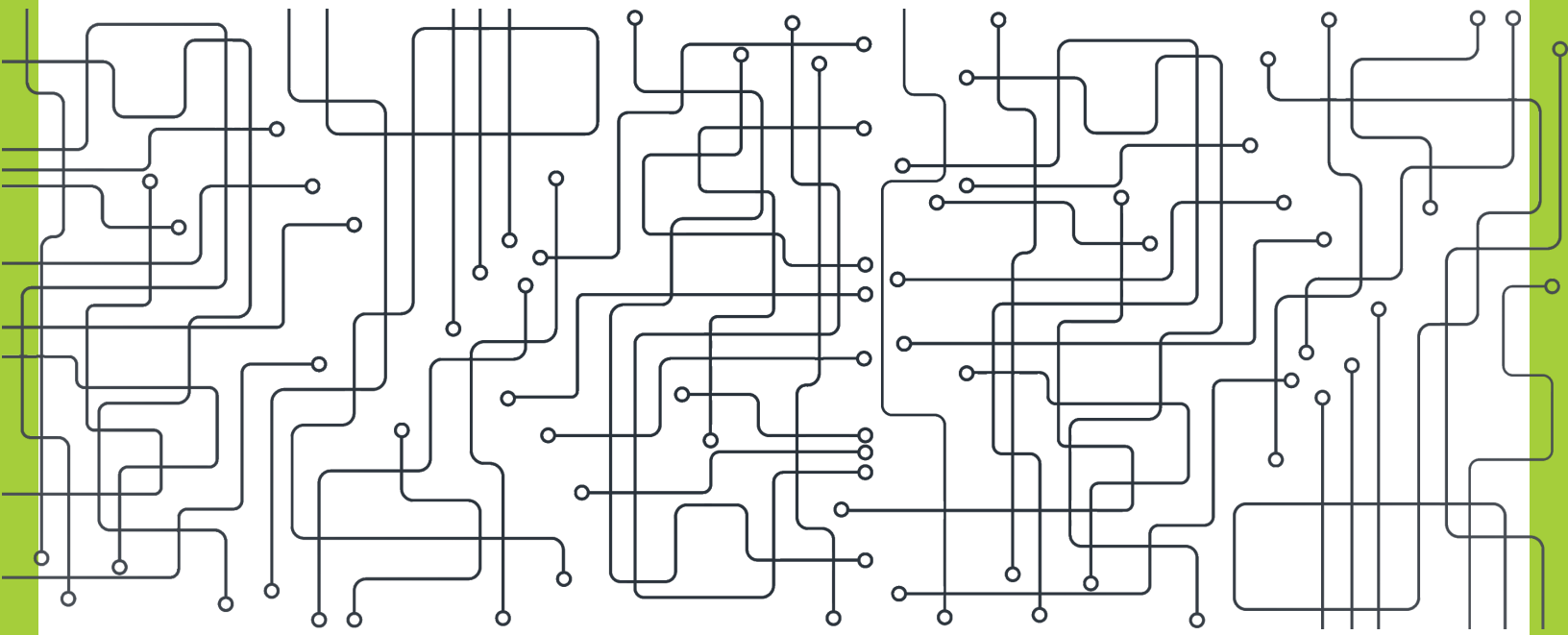
7 Does Sentinel conduct periodic cybersecurity awareness training?

Per the aforementioned tenets of the Cybersecurity Program at Sentinel, Sentinel views security as part of every employee's role. We conduct regular, required, internal cybersecurity training for every employee, organized and facilitated through Sentinel's Information Technology Team. Sentinel also sends frequent educational email campaigns to all associates to highlight best practices and tips throughout the year. In addition to these activities, Sentinel performs regular phishing awareness and training campaigns where employees are targeted with fake phishing campaigns to help practice phishing detection and identify areas for further education. One of the best weapons to protect against accidental and malicious data exfiltration is employee awareness. Sentinel recognizes this and makes training a priority of the overall cybersecurity program.



8 Has Sentinel implemented and managed a secure system development life cycle (SDLC) program?

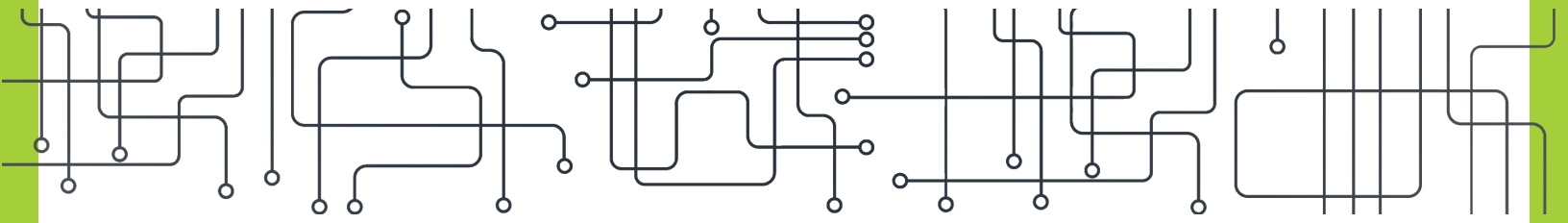
Sentinel's Information Technology Team includes a Software Development Department. As such, a SDLC program that allows for secure software production is critical. Testing, monitoring, and remediation are central to secure and functioning software, as well as a change management process for introducing any changes into the production environment. Sentinel's SDLC program has been in place for many years and its controls are part of standard day-to-day activities.



9 Does Sentinel have and maintain an effective business resiliency program addressing business continuity, disaster recovery, and incident response?

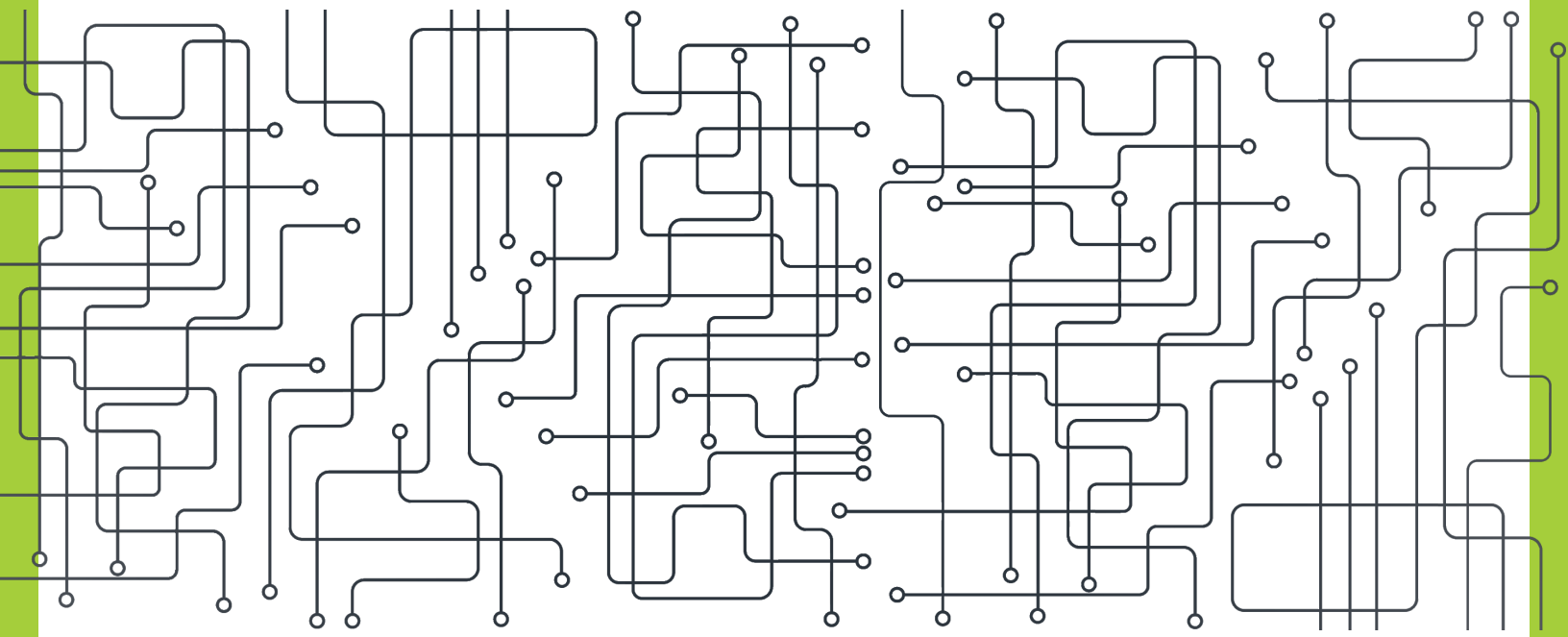
Sentinel has a well-practiced and documented Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP). Sentinel tests its BCP and DRP annually. The plans are proactively reviewed and updated as necessary whenever business operations are modified throughout the year. In addition to these plans, Sentinel is focused on continued learning on new approaches and best practices to ensure business continuity and operational resiliency as part of overall good business and cybersecurity practice.

The 2020 pandemic, and our ability to work seamlessly throughout, has in many ways been a long-term test of those capabilities. Working remotely requires virtualized technologies and digital presence solutions that are reliable, secure, and allow for employee productivity. The flexibility to operate the entire firm from anywhere, and to manage client's data, has been a demonstration of human and digital capability of our Company. Sentinel has adapted and grown the businesses' operational capabilities throughout this process.



10 Does Sentinel have privacy and security policies in place to encrypt sensitive data stored and in transit?

Sentinel has various encryption technologies that keep data safe while at rest, sitting idle and in transit. In addition to basic encryption capabilities, internal systems can detect sensitive data across the environment and report where it is and how often it's accessed. These same solutions look for encryption happening inside the environment to detect crypto virus outbreaks. Other solutions automatically encrypt email traffic when sensitive data is detected in the email contents (body, attachments, etc.) prior to it being sent.

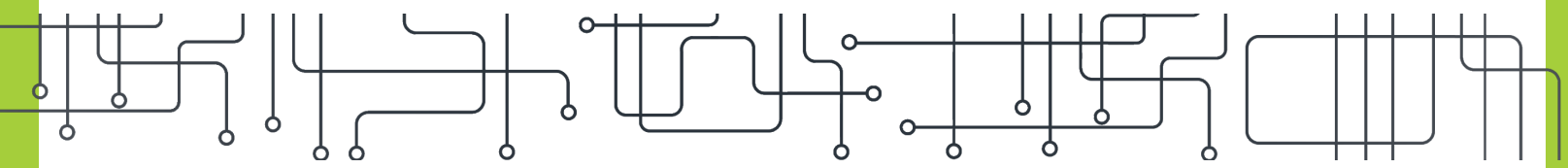


11 Does Sentinel implement strong technical controls in accordance with best security practices?

Sentinel's Information Technology Team has a number of access controls and systems for monitoring and response solutions. We employ network traffic analysis capabilities that inspect the data coming into and leaving the network, along with intrusion detection and response capabilities to stop or remediate intrusion attempts. Sentinel recognizes that using best practice Information Technology operations is critical to the overall cybersecurity program. The detection and response components of the NIST framework heavily depend on best practice processes.

Sentinel's routine technology controls include, but are not limited to:

- **Maintaining versions and updates of all software, hardware, and firmware**
- **Managing and updating firewalls and intrusion prevention and detection tools**
- **Network segregation**
- **Routine backups of databases and network data**
- **Software and infrastructure patch management**

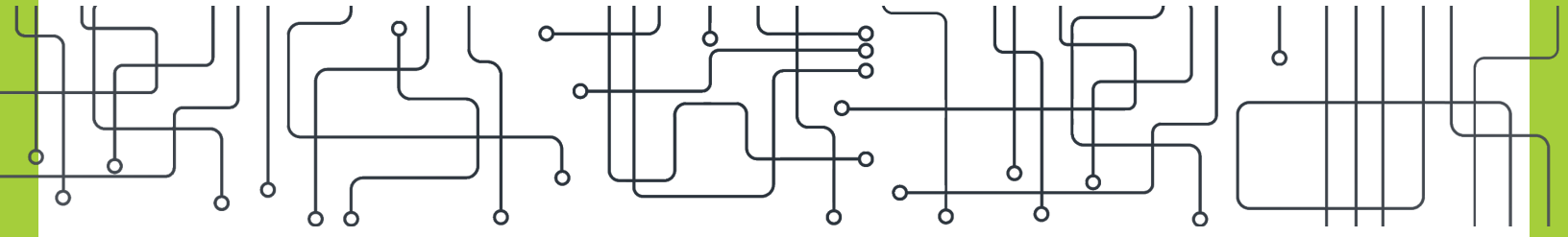


12 Does Sentinel have a process for reviewing and responding to cybersecurity incidents or breaches?

Sentinel employs a variety of technology and other controls to detect and prevent attacks based on the risk and threat to our environment.

Incident response, issue forensics, and remediation are a key component to Sentinel's cybersecurity strategy. As part of that strategy, Sentinel would review and document any occurrence of cybersecurity incidents. When potential viruses, probes and attacks happen, we believe it's important to understand the technical elements of the issue and to be able to address them from a threat perspective. Sentinel has the capability to watch and review packet level network traffic patterns to understand, and learn from, any attempted attack. Sentinel views the ability to perform this kind of analysis as critical to being able to proactively defend the environment and secure customer data.

Sentinel also maintains cybersecurity insurance coverage. In the event of an issue, Sentinel has coverage to reduce financial and business impacts.



Sentinel remains committed to safeguarding our customers from cybersecurity threats. Learn more at **www.sentinelgroup.com/Employers/Resources/Cybersecurity**.

Should have any questions, please reach out to your your dedicated Sentinel representative.