Stoneridge Cybersecurity Policy

1.0 Purpose / Scope

Cybersecurity, also known as Information Technology ("IT") Security, refers to the practice of protecting the computer, hardware, software, servers, mobile devices, electronic systems, and data from malicious attacks that will compromise the efficiency of the Company to safeguard the confidentiality and integrity of systems, applications, and information. Managing cybersecurity risk and maintaining secure, reliable, and functional corporate networks and data systems is among the highest priorities at Stoneridge. As a result, we have implemented practices, procedures, and management mechanisms to help ensure that we achieve the establishment and maintenance of a robust cybersecurity environment.

2.0 Application

The Stoneridge Cybersecurity Policy ("Policy") outlines our cybersecurity practices, procedures and management mechanisms address the prevention, detection, mitigation, and response to cybersecurity events. All Stoneridge directors, officers, employees, interns, consultants, contractors, and other third parties who interface with the Stoneridge network must fully understand and comply with this policy.

3.0 Objectives

a. Board Oversight
    i. Board-level oversight of cybersecurity matters at Stoneridge is provided by our Audit Committee, as established in the Committee's charter which is publicly available on the Stoneridge website. At least twice a year (or more often, as needed) the Committee reviews and discusses with Company management any significant information security / cybersecurity / data privacy exposures and management's plans to address and mitigate such exposures.
b. Management
    i. Stoneridge's Chief Information Officer oversees our cybersecurity practices and operations and briefs the Board's Audit Committee on cybersecurity matters twice a year (or more often, as needed). In addition, the IT team senior executive with responsibility for cybersecurity is assisted by other members of Stoneridge's IT team who are committed to cybersecurity-related operations.

c. Employees
    i. Stoneridge employees are a critical part of our defense against potential cybersecurity incident exposure. All Stoneridge employees have a responsibility and a role to play by complying with our cybersecurity operational practices and reporting any potential cybersecurity incidents or exposures to the Stoneridge IT team.
    ii. To ensure that employees can play their part in protecting the Company's networks and data from cybersecurity incident exposure, employees receive annual training on topics such as phishing, malware, and other cybersecurity risks.
d. Risk Management
    i. Stoneridge performs periodic cybersecurity risk assessments to identify, assess, and prioritize potential risks that could affect Stoneridge's information and data assets and infrastructure. If any such risks are identified, Stoneridge will address them, and controls will be developed and implemented to mitigate any issues.
    ii. Stoneridge has implemented measures to enhance the security and resiliency of our network and information/data systems. These measures include, but are not limited to:
        1. User access control management
        2. Intrusion detection and prevention systems
        3. Information security continuity measures including redundant systems and information backups
        4. Network segmentation
        5. Encryption of critical information and data
        6. Event logging
        7. Implementation of an application patching and update cadence
        8. Incident response planning

4.0 Interpretation

Any person with questions regarding the interpretation, scope, and application of this policy should contact the Stoneridge IT team.

5.0 Additional Information

This Policy is accessible on the Stoneridge website, Information Technology and Sustainability intranet sites, and is also available from Human Resources and the Compliance Department.

Report violations of this Stoneridge Policy or any law or regulation. You may report violations or suspected violations by contacting the Human Resources leader at your location, by contacting the Stoneridge Compliance Department at compliance@stoneridge.com, or through our Stoneridge Integrity Helpline by visiting www.stoneridgeintegrityhelpline.com. You may be able to make Helpline reports anonymously, where permitted by local law.

REVISION HISTORY

Rev.	Date	Description
	4/1/24	Initial release