SIGHT SCIENCES, INC.
Cybersecurity and Data Privacy

Sight Sciences, Inc. and its subsidiaries (collectively, "Sight Sciences" or the "Company") is committed to protecting our information technology (IT) systems and the data and privacy of our employees, customers, and partners through cybersecurity and privacy measures with both enterprise-wide and individual employee-level initiatives.

The Nominating and Corporate Governance Committee of the Board of Directors oversees the Company's data privacy and cyber security programs (collectively, the "Data Security Programs") cybersecurity team within the IT Department through periodic reviews at least annually of the cybersecurity practices and controls, mitigation activities, current threat levels, training initiatives, breaches, and results from any penetration testing. Cybersecurity risk management is also part of the enterprise risk management program and is reviewed by the Audit Committee at least annually.

We have developed an information security policy ensuring that our information security objectives are established and compatible with the strategic direction of the Company. The goal of this policy is to protect the Company's informational assets against reasonably foreseeable internal, external, and accidental threats. Information can exist in a variety of forms, including data that is stored on computers and associated devices, transmitted over any network infrastructure, printed on paper, sent by fax, stored on portable devices and magnetic media, or discussed during verbal or telephone conversations.

Our information security policy follows guidance from the primary global standards for security, the National Security Institute of Standards and Technology (NIST), and outlines the foundation for key components of our plan including:

- Least Privilege Access – A user is only provided the minimum access required to perform their job,
- An Incident Response Management Plan including investigation steps and notifications required on all actual and suspected information security incidents for our Security Operations Center (SOC),
- Patch Management Program to ensure that all infrastructure has the latest required patches,
- Cybersecurity training programs,
- User and Password Management including requirements for multi-Factor authentication (MFA) across all users in the organization, and
- Mandatory compliance with all cybersecurity programs, including applicable legislative and regulatory requirements.

Our Cybersecurity training program is focused on awareness of new techniques that threat actors are utilizing both in the corporate environment as well as their personal lives. The training includes both awareness videos as well as periodic Phishing, Smishing, and Vishing tests. Employees undergo regular training on information security best practices, including interactive training to confirm understanding and test skills.

The Company is committed to complying with the applicable global privacy and data security laws that govern our business operations and practices. As part of this commitment, we have taken steps to help protect the personal information we collect, use, maintain, and disclose. The Company's global privacy policy found here outlines and governs how and what information is collected, how it is used, and rights that the data subjects have to their information.

The Company provides appropriate technical and organizational measures to protect personal information from unauthorized access, use, disclosure, alteration, or destruction. Employees are trained annually on Privacy laws and the procedures and processes that they need to follow to comply with applicable regulations. We are committed to complying with data standards worldwide including, but not limited to, global privacy laws (e.g., the EU General Data Protection Regulation) and US state privacy laws (e.g., the California Consumer Privacy Act).