EYEPOINT PHARMACEUTICALS, INC.
CYBER MATERIALITY POLICY

Objectives and Scope of Policy

EyePoint Pharmaceuticals, Inc. (the "Company") as a publicly traded company has certain legal and regulatory requirements regarding the public disclosure of material information. Accordingly, the Company has developed the cyber materiality policy set out below. This cyber materiality policy (hereinafter the "Policy") has been approved by the Company's Audit Committee effective December 13, 2023.

Throughout this Policy reference is made to 17 CFR Parts 229, 232, 239, 240, and 249 [Release Nos. 33-11216; 34-97989; File No. S7-09-22] RIN 3235-AM89 Cybersecurity Risk Mange., Strategy, Governance, and Incident Disclosure, hereinafter referred to as the "SEC Rule."

This Policy outlines considerations relevant to the determination of whether a cybersecurity incident within the meaning of Item 1.05 of Form 8-K is material and therefore reportable under Item 1.05.

This Policy is not meant to be a comprehensive list of considerations, but instead to serve as a tool to memorialize a framework for the decision-making procedure that will be used in the analysis of materiality under the SEC Rule.

Materiality Determination Procedure

Per SEC Rule, the Company will follow "an informed and deliberative process" wherein, certain members of the Company Executive Team will meet and consider the relevant considerations, detailed *infra.*

Upon a notification of concerning factors which may be indicative of a Cybersecurity Incident, but, no less than monthly, the Cyber Security Subcommittee ("Cyber Security Subcommittee") consisting of the CLO, Chief People Officer, SVP of IT, Associate General Counsel, Head of Information Technology & a member of the Financial Reporting team, will make an initial assessment using the "Investment Decision" or "Total Mix of Information" tests, and express considerations, described more fully, herein. If the Cyber Security Subcommittee determines there is a reasonable likelihood a Material Cyber Incident has occurred, then notice will immediately be given and the members of the Company Executive Team considering materiality must include the following persons:

- President;
- CEO;
- CLO & Corporate Secretary;
- CFO
- Chief People Officer and SVP IT

Background & Material Cybersecurity Incident Test

Neither Item 1.05 of Form 8-K, nor any other provision of the SEC Rule contains a cybersecurity-specific materiality test. Instead, the SEC details that it expects "that registrants will apply materiality considerations [to a cyber incident] as would be applied regarding any other risk or event that a registrant faces."

The SEC Rule defines a "Material Cybersecurity Incident" as occurring where there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the 'total mix' of information made available. In keeping with same, the executive team making the materiality determination regarding whether a cybersecurity incident is a material may employ either of the following analyses:

- **Investment Decision**: there is a "substantial likelihood" that a "reasonable investor" would "consider the information important" in making an investment decision (whether to hold, buy, or sell the Company's securities).

    - The information about the incident need not actually change a reasonable investor's investment decision.
    - It is enough to show that the information would assume actual significance to a reasonable investor.

or

- **Total Mix of Information**: there is a "substantial likelihood" that a "reasonable investor" would view the information as having "significantly altered the 'total mix' of information made available."
    - The "total mix" of information refers to all information about the Company available in the public domain at the relevant time.
    - This includes information in the Company's prior SEC filings and other public communications.

Considerations in Assessing Whether the Cyber Incident was Material

Certain considerations must be reviewed in assessing whether a potential impact of the incident (e.g., exfiltration of data, loss from theft of IP) may be material, the Company should balance both (a) the probability that the impact will occur and (b) if the impact occurs, the magnitude of its expected effect on the Company, considering quantitative and qualitative factors from the perspective of a reasonable investor.

- **Quantitative Considerations:**
    - Any short- and long-term financial effects or operational effects of the incident;
    - Costs due to business interruption, decreases in production, and delays in product launches;
    - Ransom or other payments to the cyber intruders;

- Lost revenues resulting from IP theft and unauthorized use of proprietary information or failure to retain or attract customers;
- Liabilities to affected parties;
- Increased costs of capital;
- Diminished cash flows;
- Data theft;
- Loss of IP or other assets;
- Asset impairments;
- Remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners to maintain relationships;
- Increased cybersecurity protection costs, including increased insurance premiums and costs of organizational changes and engagement of third-party experts and consultants.

- **Qualitative Considerations:**
  - Reputational harm;
  - Damage to brand perception;
  - Harm to customer or vendor relationships;
  - Diminished competitiveness;
  - Damage to the Company's stock price and long-term shareholder value;
  - Possibility of litigation or regulatory investigations or actions by state and federal and non-U.S. governmental authorities;
  - Theft of information that may be deemed not material based solely on quantitative financial measures, but that could adversely affect the Company because of the scope or nature of harm to individuals, customers, or others.

- **Additional Considerations**
  - Potential impact of disclosure on stock price;
  - Company's prior public disclosures;
  - Reporting decisions by other affected companies;
  - Company determinations for prior similar incidents;
  - Market disclosure practice for similar incidents;
  - Market reaction to similar incidents.

Timing

The SEC requires determination of the materiality of an incident "without unreasonable delay following discovery" and, if the incident is determined material, to file an Item 1.05 Form 8-K within four business days of such determination.

- If an incident is deemed Material, the Company will not delay the filing of its initial Item 1.05 Form 8-K report until it completes its ongoing internal or external investigation of the

incident; or until it mitigates, contains, remediates, or otherwise diminishes the incident's adverse impacts.

- The Company will continue to consider additional information and either amend/update a prior disclosure, or publish a new disclosure within 4 days of new, material, information being presented.

Review of Company Cyber Materiality Policy

The Audit Committee shall annually review this policy.