

**Primoris Services Corporation
Security Steering Committee Charter
June 2022**

I. Risk Management, Security Steering Committee

The Security Steering Committee (“SSC”) is comprised of cybersecurity strategy and risk experts and maintains the policies and awareness of threats and vulnerabilities on an ongoing basis. Further, the SSC educates employees regarding cybersecurity using security awareness training, security bulletins and phishing simulations to reinforce training on a quarterly basis. Cybersecurity training is made available to all employees with Primoris network accounts through an online training portal.

Primoris conducts vulnerability scans and penetration testing and works with third-parties to perform baseline assessments of the cyber program that measures improvement and provides feedback on the Company’s incident response plan and related solutions. The National Institute of Science and Technology (NIST) Cybersecurity Framework is the basis for the Company’s cybersecurity framework, and on a regular basis, the Audit Committee of the Board of Directors reviews and discusses any key issues related to information technology, cybersecurity risks and management programs.

II. Purpose

Primoris Services Corporation (“PSC” or the “Company”) believes that maintaining security of information and mitigating against cyber risk is vital to maintaining our proprietary and confidential information and the trust of our employees, customers and supply chain.

In combination with the Executive Committee and the Company’s Board of Directors (the “Board”), the SSC has oversight responsibility to provide and maintain a comprehensive cybersecurity program to protect PSC’s information technology environment, including but not limited to data governance, privacy and compliance.

Our cybersecurity awareness training program includes modules covering key risk topics such as but not limited to information, phishing/smishing, password management, and malware.

III. Executive Committee

The Executive Committee (“Executive Committee”) consists of the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer and Chief Legal Officer.

- a) The Executive Committee is responsible for reporting to the Audit Committee of the Board of Directors and the Board on matters of cyber safety and strategy to mitigate risks; and the progress of the SSC. The Audit Committee of the Board of Directors has compliance oversight for matters of Information Technology risks including cybersecurity risks.

- b) The Board receives quarterly updates that include information about cybersecurity governance processes, the status of projects to strengthen internal cybersecurity, and the results of security breach simulations.

IV. Membership

The members of the SSC includes the Senior Vice President Information Technology; the Senior Vice President Human Resources; and such officers and employees of the Company deemed appropriate, taking into account such person's expertise in relevant disciplines such as information systems, corporate governance, finance, legal, human resources and operations.

- a) The SSC meets quarterly and reports to the Executive Committee. In addition to quarterly meetings, the frequency of SSC meetings is determined by specific projects on a weekly, bi-weekly, monthly; or risk-by-risk basis.

V. Performance Objectives

- a) No cybersecurity breaches of PSC intellectual property, actual or simulated
- b) Agreed upon cybersecurity strategy, roadmap & supporting initiatives
- c) Successful completion of security initiatives, IT Controls Audits, and cybersecurity assessments against externally established frameworks (i.e., National Institute for Standards and Technology)

VI. Duties and Responsibilities

- a) *Data Governance* – To provide oversight of policies, procedures, plans and execution intended to provide security, confidentiality, availability and integrity of the information.
- b) *Awareness* – Ensure overall cybersecurity awareness and priority at all levels of PSC, including external cybersecurity threats and breaches in the marketplace.
- c) *Information Technology Systems* – To oversee the quality and effectiveness of the Company's policies and procedures with respect to its information technology systems, including privacy, network security and data security.
- d) *Incident Response* – To review and provide oversight on the policies and procedures of the Company in preparation for responding to any material incidents, including overall governance in the event of a cybersecurity breach.
- e) *Disaster Recovery* – To review periodically with management the Company's disaster recovery capabilities.
- f) *Compliance Risks and Internal Audits* – To oversee the Company's management of risks related to its information technology systems and processes, including privacy, network security and data security, and any internal audits of such systems and processes.
- g) *IT Security Budget* – To oversee the Company's information technology senior management team relating to budgetary priorities based, in part, on assessing risk associated with various perceived threats, including initiatives, staffing and use of external partners.
- h) *Sounding board* – for PSC Board of Directors requests and meetings; results of risk audits are reported to leadership and the applicable Board committee as appropriate.