IT RISK GOVERNANCE POLICY

POLICY STATEMENT

Robinsons Retail Holdings, Inc. (“RRHI”, the “Company”) recognizes the critical importance of cybersecurity controls in maintaining a robust organizational security posture.

OBJECTIVE

The IT Risk Governance Policy (the “Policy”) establishes a proactive and collaborative framework that effectively identifies, manages, and mitigates cybersecurity risks. By aligning with industry best practices, regulatory requirements, and fostering a culture of security, the Company aims to safeguard its assets and information, ensuring the resilience of its IT infrastructure against evolving threats.

SCOPE AND COVERAGE

This Policy applies to all directors, officers, employees, contractors, and third-party entities with access to RRHI's information systems and assets. It encompasses all IT resources, including hardware, software, networks, and data owned or managed by the Company. To effectively manage and mitigate IT risks, the Company adheres to established cybersecurity frameworks such as the National Institute of Standards and Technology (“NIST”) and International Organization for Standardization (“ISO”).

GENERAL POLICIES

The general policies are as follows:

1. The Company employs a layered approach to security controls, encompassing both physical and technical measures. This includes access controls, surveillance cameras, firewalls, intrusion detection systems, and endpoint protection software, creating a comprehensive and resilient security system.

2. Regular testing and monitoring of security controls are conducted to ensure their ongoing effectiveness. This involves penetration testing, vulnerability scanning, and security assessments. Continuous monitoring of security logs and alerts is implemented to detect and address potential security incidents promptly. This allows the Company to identify and address weaknesses in the security system, thereby reducing the risk of a successful cyberattack or data breach.

Risk Management Best Practices

3. Effective management and reporting of identified security risks require a proactive and collaborative approach. The Information Security Office (ISO) regularly reviews and updates risk management practices to adapt to the evolving threat landscape and changes within the Company.

   To effectively manage and report identified cyber security risks, the ISO adheres to the following best practices:

   3.1. Prioritize identified security risks based on their potential impact and likelihood of occurrence and focuses on addressing high-priority risks first to mitigate the most significant threats to the Company.

   3.2. Develop and implement risk mitigation strategies for each identified risk. Determine appropriate controls, safeguards, and countermeasures to reduce the likelihood and impact of the risks. Align these strategies with industry best practices, regulatory requirements, and to the Company's risk appetite.

3.3. Information Security Incident Response Plan that outlines the steps to be taken in the event of a security incident related to the identified risks. Define roles and responsibilities, communication channels, and escalation procedures. Regularly test and update the plan to ensure its effectiveness.

3.4. A continuous monitoring program to detect and respond to security incidents and changes in risk levels. Monitor security controls, conduct vulnerability assessments, and analyze security logs and alerts. Proactively identify and address emerging risks and vulnerabilities.

3.5. Establishment of a robust reporting mechanism to communicate identified security risks to relevant stakeholders. Prepare clear and concise risk reports that provide an overview of the risks, their potential impact, and the status of risk mitigation efforts.

3.6. Define clear and relevant metrics and KPIs to measure the effectiveness of risk management efforts. Track and report on these metrics regularly to assess the progress in mitigating identified risks. This helps in demonstrating the Company's commitment to security and provides insights for continuous improvement.

3.7. Conduct periodic risk reviews to reassess identified risks, evaluate the effectiveness of risk mitigation strategies, and identify emerging risks. Incorporate feedback from security incidents, audits, and assessments into the risk management process. Use the findings to refine risk mitigation strategies and enhance security controls.

3.8. Educate employees about the identified security risks, their potential impact, and their role in mitigating those risks. Provide regular training sessions and awareness programs to promote a culture of security within the Company. Encourage employees to report security incidents or potential risks promptly.

EFFECTIVITY

This Policy shall take effect upon approval and shall continue to be in full force unless superseded by new policies and guidelines.

-o0o-