veris
RESIDENTIAL

CYBERSECURITY FRAMEWORK: SAFEGUARDING INFORMATION ASSETS AND BUSINESS OPERATIONS

PURPOSE

This Cybersecurity Framework is established to protect the integrity, confidentiality, and availability of the Company's information technology systems, proprietary and confidential information, and the personal data of tenants, business partners, and employees. The framework reflects a commitment to robust cybersecurity practices, continuous risk assessment, and a strategic approach to evolving cyber threats.

SCOPE

This framework applies to all Company information technology resources, including communication networks, system applications, data centers, third-party hosted services, and all hardware and software platforms. It governs all employees, contractors, and third-party vendors with access to Company data and systems.

CYBERSECURITY STRATEGY

- The Company employs a multi-faceted cybersecurity strategy focused on detection, protection, incident response, risk management, and resilience.
- Key security measures include data encryption, frequent password changes, firewall and intrusion detection systems, anti-virus software, frequent data backups, and consultation with external cybersecurity experts.
- Internal controls are implemented for treasury functions, including enhanced payment authorizations, vendor verification, and rigorous reconciliation procedures.
- Comprehensive policies and procedures are in place for the identification, escalation, and remediation of cybersecurity incidents.
- Physical, administrative, and technical safeguards are used across all critical assets.
- Regular employee cybersecurity training and periodic testing of employee awareness are required.

RISK ASSESSMENT AND MANAGEMENT

- The Company leverages the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) to evaluate and report on the maturity of cybersecurity controls.
- Third-party technical assessments and reviews of IT architecture are conducted regularly.
- Vendor management procedures include cybersecurity evaluations, contractual obligations, and periodic reassessment of third-party providers, with scope and depth appropriate to the sensitivity of data and services.
- The Company maintains an evolving, multi-year cybersecurity plan to enhance and fortify security defenses in response to shifting threats and operational requirements.

ROLES AND RESPONSIBILITIES

- The Chief Information Security Officer (CISO), reporting to the Chief Operating Officer, leads cybersecurity risk management and implementation of security measures. The CISO brings over 30 years of experience, including within highly regulated industries.
- A cross-functional Cyber ERM (Enterprise Risk Management) Committee oversees incident response and ensures rapid escalation and coordinated action in the event of a cybersecurity incident.
- All employees are responsible for complying with this framework, completing cybersecurity training, and reporting suspicious activities or incidents promptly.
- The Audit Committee of the Board oversees cybersecurity strategy and risk, receiving regular and ad hoc reports from executive management and the CISO.

INCIDENT RESPONSE AND REPORTING

- Incident identification, reporting, and escalation procedures are in place to ensure timely response to any threat or breach.
- The Cyber ERM Committee is responsible for implementing rapid response actions and reporting material incidents to the Audit Committee and Board of Directors.
- Material incidents are evaluated for regulatory and reporting obligations in accordance with applicable laws and the Exchange Act.

CONTINUOUS IMPROVEMENT

- The Company is committed to continuous evaluation, testing, and updating of cybersecurity processes and technologies.
- Assess adoption of NIST CSF 2.0
- Regular reassessment of the risk environment and adoption of industry best practices inform the ongoing development of cybersecurity defenses and employee training.
- The Company is not aware of any past or present cybersecurity threats or incidents that have had, or are reasonably likely to have, a material impact on its business, strategy, or financial condition. This framework will be reviewed and updated as needed to reflect the changing cybersecurity landscape.