NEWMARK GROUP, INC.
CYBER-SECURITY PROGRAM POLICY STATEMENT

Newmark Group, Inc. ("Newmark") has approved the following global policy with respect to Newmark and its subsidiaries on a global basis .

The following policy reflects its commitment to cyber-security on a global basis with respect to all subsidiaries and business lines and forms part of its governance standards.

Commitment

Newmark is committed on a global basis to combatting the global threat of cyber-security and to securing its business to operate with confidence, through a deep understanding of cyber risks, vulnerabilities, mitigations, and threats.

Program Measures

Newmark's cyber-security program supports the following organizational missions:

- Protect the Company's people, technology and assets from outside threats
- Protect the Company's data from accidental and malicious disclosure
- Protect the Company from insider threats

The program has been established under an umbrella of current global policies and standards, including ISO-27000 and NIST-800. Controls are framed through the CIS20 and their effectiveness is illustrated via the NIST CSF. The program is updated and revised frequently in response to evolving global standards and events.

Governance

The Information Security Group is led by Newmark's Chief Information Security Officer (the "CISO"), who reports to senior management frequently and to the Company's Board of Directors on a periodic basis. The CISO provides governance for all information security matters, including priorities, setting the supporting strategies and developing the Information Security Group to deliver the cyber-security program.

The Information Security Group provides cyber defense, operations, architecture, engineering, cyber risk and threat management. The Information Security Group also engages in:

- Regular liaisons with industry and government to keep pace with the evolving threats;
- Periodic internal and external vulnerability audits and assessments and penetration testing;
- Expert third parties to evaluate and monitor the effectiveness of the program; and
- Developing policies, documented operational procedures and regular cybersecurity employee, contractor and Board training globally.

Version: September 2021