



Cybersecurity Policy

As we increasingly rely on information technology to manage our business and the safety of our operations, our processes and networks may be vulnerable to information risks, including unauthorized access, malware, theft and other cybersecurity events that could adversely affect our business, results from operations and financial condition. The nature of this threat is continually changing and is expected to intensify as the cyber threat landscape evolves and becomes more sophisticated.

To address these risks, we have invested in security resources and maintain a robust cybersecurity program to deliver on the following commitments:

- Implement and maintain appropriate systems and processes to protect our infrastructure from cybersecurity risks.
- Address evolving threats through threat detection and cyber assurance activities.
- Continuously monitor and periodically test our readiness to address cybersecurity events.
- Develop and maintain appropriate incident response processes and the necessary resources and expertise to respond to detected threats and recover as quickly as possible from cybersecurity breaches.
- Hold management of Exchange Income Corporation and its subsidiaries accountable for providing leadership on cybersecurity matters.
- Communicate with our employees about their responsibilities and provide necessary training and awareness programs.

Oversight and coordination of data privacy and cyber security matters is the responsibility of the Audit Committee of Exchange Income Corporation's Board of Directors.