Rexford Industrial Realty
Cybersecurity Policy

The following cyber security policy outlines Rexford Industrial Realty, Inc.'s ("Rexford") policy for preserving the security of our data and technology infrastructure. This policy applies to all employees, contractors and vendors or other persons that have, or may require, access to information and information technology ("IT") resources at Rexford.

Rexford has implemented extensive internal cybersecurity policies that are not available for public reference. The following policy provides important aspects of Rexford's approach to managing cybersecurity but should not be viewed as an all-encompassing document.

The Head of IT is responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be approved, mandated and/or endorsed by management where applicable (the "IT Policies"). Working in conjunction with other corporate functions, IT is also responsible for conducting suitable awareness, training and educational activities to raise awareness and aid understanding of staff's responsibilities identified in applicable policies, laws, regulations, contracts, etc. Rexford management is responsible for oversight and enforcement of the IT Policies.

Security Awareness Training and Testing

Technical security controls are a vital part of our information security framework but are not in themselves sufficient to secure all information assets. Effective information security also requires the awareness and proactive support of all staff, supplementing and making full use of the technical security controls. In order to protect information assets, it is our policy that all workers must be informed about relevant, current information security matters, and must be motivated to fulfill their information security obligations. Rexford's information security awareness program strives to ensure that all staff achieve and maintain at least a basic level of understanding of information security matters. All staff are personally accountable for completing the security awareness training activities and complying with applicable policies, laws and regulations at all times.

Incident Management Handling and Response Framework

All persons accessing and using Rexford's Information Technology resources have a responsibility to immediately report any suspected security incidents to the Rexford Help Desk. Upon notification of an incident, Rexford works to identify if a system's resource has been compromised, to limit the exposure of sensitive data, to clean the resource(s), and to determine if

breach notification is required. Breach communications will be handled in accordance with applicable state and federal laws.

Enforcement

Violation of the policies detailed within this document could result in disciplinary actions up to and including termination with legal prosecution.

This Cybersecurity Policy was approved and made effective by the Rexford Board of Directors on April 19, 2021.