Rexford Industrial

# Rexford Industrial Realty
# Cybersecurity Policy

## Introduction

This Cybersecurity Policy outlines Rexford Industrial Realty, Inc.'s ("Rexford") approach to safeguarding our data and technology infrastructure. It applies to all employees, contractors, vendors, and any individuals requiring access to Rexford's Information Technology ("IT") resources.

Rexford has implemented comprehensive internal cybersecurity policies that are not publicly available. This document highlights key aspects of our approach to cybersecurity and Artificial Intelligence (AI) approach but is not exhaustive.

## Roles and Responsibilities

- **Head of Technology**: Responsible for creating, maintaining, and updating Rexford's IT policies, ensuring alignment with regulatory requirements and internal standards.
- **IT Department**: In collaboration with other corporate functions, conducts awareness training, and educational activities to ensure staff understand their responsibilities under applicable policies, laws, regulations, and contracts.
- **Director of Cybersecurity and Technology Operations**: Oversees Rexford's cybersecurity efforts and ensures compliance with IT policies in collaboration with other members of management.

## Commitment to Responsible AI Use

At Rexford, we recognize the transformative potential of AI in driving innovation and operational efficiency. We are committed to the ethical and responsible use of AI, ensuring respect for data privacy, cybersecurity, and fairness in all AI-related activities. Our AI policy prioritizes the protection of personal and company information, enhances transparency in AI-generated content, and strives to mitigate any potential biases in AI outputs. It complements our cybersecurity policies and underscores Rexford's commitment to ethical, transparent, and secure AI practices.

Our approach to responsible AI is guided by the principles outlined in the NIST AI Risk Management Framework, and we are actively building toward full alignment:

1. **Govern:** Rexford has established oversight for AI initiatives and is defining roles and responsibilities to ensure accountability. Documentation practices are evolving to support audits and regulatory readiness.
2. **Map:** We review AI use cases for potential risks—such as bias, privacy, and cybersecurity—prior to deployment and continue to refine these processes.
3. **Measure:** Monitoring for performance, fairness, and security is in progress, with plans to expand assessments and audits as our program matures.
4. **Manage:** Training on responsible AI practices is being introduced, and AI systems follow security protocols (e.g., encryption, access controls) to prevent misuse and strengthen resilience against AI-enabled threats.

### Security Awareness Training and Testing

Rexford's security awareness program ensures all staff understand and comply with information security obligations. All employees are accountable for completing required training and adhering to applicable policies, laws, and regulations at all times.

### Incident Management Handling and Response Framework

All individuals accessing Rexford's IT resources must immediately report any suspected security incidents to the Rexford Help Desk. Upon notification, Rexford will identify compromised systems, limit data exposure, remediate affected resources, and determine if breach notification is required, in accordance with applicable state and federal laws. To ensure preparedness, Rexford tests its business continuity plan and incident response procedures at least annually.

### Enforcement

Violations of these policies, such as unauthorized access, failure to complete training, or negligent handling of sensitive data, may result in disciplinary actions, up to and including termination, and could lead to legal prosecution.

This Policy was approved and made effective by the Rexford Board of Directors on April 19, 2021; last updated February 27, 2026.