Cybersecurity Policy – Rivendell Supply Co.

(A Fictional logistics and supply company, ~200 employees)

Executive Summary

This policy outlines key cybersecurity requirements for **Rivendell Supply Co.** to protect company assets, maintain compliance with industry standards, and safeguard customer data. Each policy has been researched to be aligned with the NIST Cybersecurity Framework (CSF) to ensure a structured approach and understanding in risk management. With a workforce of approximately 200 employees across multiple sites, including remote locations, Rivendell Supply Co. will require standardized security practices to reduce risks and ensure business continuity.

---

1. Acceptable Use Policy (AUP)

- All company-owned devices, accounts, and networks are to be used solely for authorized business purposes.
- Employees must not install unauthorized software, access prohibited websites, or engage in activities that could compromise security.
- Monitoring of device usage will be continuously conducted to ensure compliance with AUP.
- Department managers are responsible for reviewing access privileges quarterly.

---

2. Password Management Policy

- All user accounts must be secured with unique, complex passwords (minimum 12 characters).
- Multi-factor authentication (MFA) is required for all remote access, privileged accounts, and cloud applications.
- Passwords must be rotated every 90 days and stored only in an approved password manager.
- Shared accounts are prohibited unless approved by IT Security with additional controls.

- Privileged Access Management (PAM) tools must be used for administrator accounts.

---

3. Incident Response Policy

- All suspected or confirmed security incidents must be reported immediately to the IT Security Team via the incident hotline or secure ticketing system.
- The IT Security Team will assess, contain, and escalate incidents according to the documented incident response plan.
- A designated Incident Response (IR) team will include IT, Legal, HR, and Communications for coordinated response.
- Post-incident reviews must be conducted within 10 business days to ensure lessons learned are captured.

---

4. Data Protection Policy

- Sensitive customer, employee, and business data must be encrypted both in transit (TLS 1.2 or higher) and at rest (AES-256 standard).
- Backups must be performed daily, tested monthly, and stored securely offsite or in an encrypted cloud environment.
- Access to sensitive data is restricted to business-justified roles and reviewed quarterly by management.
- Data Loss Prevention (DLP) solutions must be implemented to monitor and protect sensitive data movement.

---

5. Remote Work Security Policy

- Remote employees must connect via a company-approved VPN.
- Endpoint devices must be patched, protected by EDR/AV software, and comply with company configuration baselines.
- Public Wi-Fi must not be used without VPN protection.

- Personally owned devices may only be used if they meet security standards and are enrolled in the company's Mobile Device Management (MDM) system.
- Remote work compliance audits will be conducted biannually.