Date: [Insert Date]

To: All Department Heads and Procurement Officers

From: [Insert Name/Department, e.g., Office of Risk Management]

Subject: DIRECTIVE: Implementation of New Vendor Risk Management (VRM) Compliance Standards

Effective [Insert Effective Date], [Company Name] is implementing updated Vendor Risk Management (VRM) Compliance Standards. These new protocols are mandatory for all current and future third-party engagements.

1. Purpose
The objective of these standards is to mitigate operational, financial, and cybersecurity risks associated with third-party vendors and to ensure alignment with current regulatory requirements.

2. Key Compliance Requirements

- **Risk Tiering:** All vendors must be categorized as High, Medium, or Low risk based on the data they access and the criticality of their service.
- **Due Diligence:** No contract shall be signed or renewed without a completed Security and Compliance Assessment.
- **Continuous Monitoring:** High-risk vendors are now subject to [Insert Frequency, e.g., semi-annual] performance and security audits.
- **Standardized Contract Clauses:** All agreements must include the updated "Data Protection and Liability" clauses provided by the Legal Department.

3. Action Required

All personnel involved in vendor selection or management must:

1. Review the full VRM Policy attached to this directive.
2. Ensure all active vendors in your department have a completed risk profile on file by [Insert Deadline Date].
3. Attend the mandatory training session scheduled for [Insert Date/Time].

4. Enforcement
Failure to comply with these standards may result in the suspension of vendor payments or the termination of existing service agreements.

Please direct any questions regarding the assessment process to the Risk Management Team at [Insert Email/Phone].

Sincerely,

[Signature]

[Insert Name]
[Insert Title]