To: All Branch Managers

From: [Your Name/Department]

Date: [Insert Date]

Subject: INSTRUCTIONAL: Updated Vendor Risk Management Policy Compliance

Dear Branch Manager,

This letter serves as formal notification regarding updates to the company's Vendor Risk Management (VRM) Policy. To ensure organizational security and regulatory compliance, all branches are required to implement the following procedural changes effective [Insert Date].

Required Actions:

- **Inventory Review:** Audit all current third-party service providers at your branch. Ensure every vendor is documented in the central portal.
- **Risk Tiering:** Categorize each vendor as High, Medium, or Low risk based on their access to customer data or physical branch premises.
- **Due Diligence Documentation:** Collect updated business licenses and insurance certificates for any vendor categorized as Medium or High risk.
- **Reporting:** Submit your completed Branch Vendor Log to the Compliance Department no later than [Insert Deadline].

Policy Key Changes:

The updated policy now mandates that no new vendor contracts may be signed at the branch level without a preliminary cybersecurity screening. Furthermore, any vendor with onsite access must now undergo a background verification process coordinated through Corporate Security.

Support and Resources:

A full copy of the revised policy and the new screening templates can be found on the company intranet under the "Compliance" tab. If you require assistance with the classification of a specific vendor, please contact the Risk Management Team at [Insert Phone Number/Email].

Thank you for your immediate attention to these security protocols.

Sincerely,

[Your Signature]
[Your Title]
[Company Name]