Date: [Insert Date]

To: [Name of Responsible Officer/Department Head]
From: [Name of Supervisor/Information Security Officer]
Subject: SUPERVISORY LETTER: Cybersecurity Vulnerability Remediation Requirement

Dear [Recipient Name],

This letter serves as a formal notification regarding critical cybersecurity vulnerabilities identified within your department's managed systems. A recent security assessment has flagged the following risks that require immediate attention:

- **Vulnerability ID:** [e.g., CVE-2023-XXXXX]
- **Affected Systems:** [Insert System Names/IP Addresses]
- **Risk Severity:** [Critical/High]
- **Potential Impact:** [e.g., Unauthorized Data Access / System Compromise]

In accordance with the Organization's Cybersecurity Policy, you are required to initiate remediation actions immediately. Please adhere to the following timeline:

1. **Acknowledgement:** Confirm receipt of this letter and designate a technical lead by [Insert Date/Time].
2. **Remediation Plan:** Submit a brief plan of action, including patching or mitigation steps, by [Insert Date].
3. **Completion:** Final remediation and verification testing must be completed no later than [Insert Date].

Failure to address these vulnerabilities within the specified timeframe may result in the temporary suspension of the affected services to protect the integrity of the corporate network.

If there are operational constraints preventing immediate patching, a formal "Risk Acceptance" or "Compensating Control" request must be submitted to the Information Security Office for review.

Please contact [Insert Name/Department] at [Insert Email/Phone] for technical assistance or clarification regarding these findings.

Regards,

[Signature]
[Name of Supervisor]
[Title]
[Department]