Date: [Insert Date]

To: [Insert Name/Department]

From: [Insert Name/Title]

Subject: Feedback on Cybersecurity Incident Response Resilience

Dear [Insert Name],

Following the recent cybersecurity incident involving [Insert Brief Incident Description/Reference Number], we have completed a review of our response performance and overall system resilience.

1. Executive Summary:
The primary objective of this feedback is to identify strengths and weaknesses encountered during the containment, eradication, and recovery phases of the incident.

2. Key Strengths Observed:

- [Insert Strength, e.g., Rapid detection by monitoring tools]
- [Insert Strength, e.g., Effective communication across internal teams]
- [Insert Strength, e.g., Successful restoration from backups]

3. Areas for Improvement:

- [Insert Gap, e.g., Delay in third-party vendor notification]
- [Insert Gap, e.g., Lack of clarity in the incident escalation chain]
- [Insert Gap, e.g., Insufficient documentation during the live response]

4. Resilience Recommendations:

- [Insert Recommendation, e.g., Update Incident Response Plan (IRP) documentation]
- [Insert Recommendation, e.g., Schedule quarterly tabletop exercises]
- [Insert Recommendation, e.g., Implement automated alerting for specific sub-systems]

5. Conclusion:
The goal of these findings is to strengthen our defensive posture and ensure a more robust response to future threats. We request that the relevant stakeholders review these points and provide a timeline for the implementation of the recommended improvements by [Insert Date].

Sincerely,

[Your Signature]
[Your Printed Name]
[Your Job Title]