Date: [Insert Date]

To: [Recipient Name/Department]

From: [Your Name/Incident Response Team]

Subject: Report on Internal Containment and Remediation Measures Executed

Dear [Recipient Name],

This document serves as a formal summary of the containment and remediation actions taken following the identification of the security incident on [Incident Date].

1. Containment Measures

Upon detection, the following steps were executed to limit the scope of the incident and prevent further impact:

- **Isolation:** [e.g., Affected servers/workstations were disconnected from the network].
- **Account Suspension:** [e.g., Compromised user credentials and administrative access were disabled].
- **Traffic Filtering:** [e.g., Inbound/outbound traffic to known malicious IP addresses was blocked].

2. Remediation Actions

To restore system integrity and eliminate the root cause, the following remediation measures were completed:

- **Threat Removal:** [e.g., Malware was quarantined and deleted from all affected endpoints].
- **Vulnerability Patching:** [e.g., Security patches were applied to address the exploit used in the breach].
- **System Restoration:** [e.g., Impacted systems were rebuilt from verified clean backups].
- **Credential Reset:** [e.g., A mandatory password reset was enforced across the affected business unit].

3. Verification and Monitoring

Post-remediation, the internal environment was subjected to the following verification processes:

- Scanning of systems to ensure no residual indicators of compromise (IoCs) remain.
- Increased logging and 24/7 monitoring of the affected network segments.
- Validation of data integrity for all restored services.

The incident is currently classified as [Contained/Resolved]. We are continuing to monitor the situation to ensure long-term stability.

Sincerely,

[Your Signature]
[Your Title]
[Organization Name]