LOTUSCARE SERVICES
Internal Incident Update – Day 1
CONFIDENTIAL – Executive Circulation Only

Date: [redacted]/[redacted]/2026

1. Incident Summary

At approximately 08:42 AEST, multiple users reported inability to access shared files.
Initial investigation indicates widespread encryption of workstation and server files consistent with ransomware activity.

A ransom note was deployed across affected endpoints.

2. Scope of Impact

- 47 user workstations encrypted
- Primary file server impacted
- Access to shared drives disrupted
- Email services operational
- Domain controller status under review

3. Initial Access Vector (Preliminary)

Forensic indicators suggest initial compromise likely occurred via malicious file execution by a staff member in the Finance division.

Evidence indicates macro-enabled document execution consistent with known ransomware loader techniques.

Investigation ongoing.

4. Lateral Movement & Automation

Indicators show rapid credential harvesting and automated lateral spread across the internal network.

Encryption began within approximately 18 minutes of initial execution.

This suggests use of automated deployment tooling rather than manual intrusion.

5. Backup Status

- Last verified full backup: 72 hours prior
- Shadow copies deleted on multiple endpoints
- Integrity of backup environment currently being assessed

6. Data Exfiltration

Outbound network traffic spikes observed prior to encryption event.

Data exfiltration cannot be ruled out.

7. Immediate Actions Taken

- Network segmentation initiated
- External IR consultants engaged
- Law enforcement notified
- Systems isolated from internet

Further updates to follow.

Kim Young

Head of IT Security