Incident Response Plan – SecureNet Ltd

Purpose:
This plan outlines how SecureNet Ltd responds to cybersecurity incidents to minimize damage and recovery time.

1. Preparation:
Maintain updated contact list, perform regular backups, and conduct awareness training.

2. Identification:
Detect and log any unusual activity, alerts, or security events.

3. Containment:
Isolate affected systems and prevent lateral movement across the network.

4. Eradication:
Remove malicious software, disable compromised accounts, and patch vulnerabilities.

5. Recovery:
Restore affected systems from clean backups and monitor for recurring issues.

6. Lessons Learned:
Conduct a post-incident review and update policies to prevent recurrence.

Contact Information:
Security Team Email: security@securenet.com | Hotline: +44 7000 000 000