

Information Security Handbook

1. Incident Response

All suspected security incidents must be reported to the Security Operations team immediately through the incident channel. Employees should not investigate independently.

1.1 Triage Timelines

Critical incidents require initial triage within 15 minutes of being reported. High severity incidents require triage within one hour, and all other incidents within one business day.

2. Device Security

Company-managed devices must use full-disk encryption, automatic screen locking after five minutes, and multi-factor authentication for all cloud service logins.

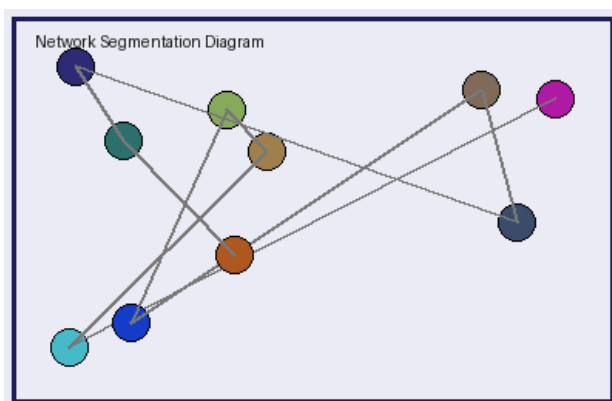


Figure 1 shows the reference network segmentation diagram.

2.1 Encryption Standards

Disk encryption must use AES-256 or equivalent. Key material must be stored in a hardware-backed keystore where the device supports one, and rotated on a 12 month cycle.

3. Access Control

Access to production systems requires multi-factor authentication and is reviewed quarterly by the security team.