Information Security Policy - Compliant Version

1. Authentication and Password Management: All users must keep passwords secure, must not share accounts, and must follow multi-factor authentication requirements.

2. Access Control: Access to systems and data will be limited based on roles and responsibilities, with periodic access reviews.

3. Information Classification: All data must be classified (Confidential, Internal, Public) and appropriately labeled.

4. Encryption: Sensitive data, including NCIC and CJIS information, must be encrypted in transit and at rest.

5. Incident Response: Security incidents must be reported immediately, with an established escalation and response process.

6. Business Continuity: Information security must be maintained during disruptions through defined continuity and recovery plans.

7. Security Training: Employees must undergo regular training on security awareness and responsibilities.

8. Vulnerability Management: Regular vulnerability scans must be performed, and security patches applied in a timely manner.