Security and Ethical Issues in AIS

Security and Ethical Issues in AIS

1. **Data Security Risks**
    - Unauthorized access, hacking, data breaches, and insider threats can compromise sensitive financial and personal data.
2. **Key Security Measures**
    - Access controls (usernames/passwords, role-based permissions), encryption, firewalls, and regular security audits.
3. **Business Continuity**
    - Backup systems and disaster recovery plans ensure the AIS can be restored quickly after a system failure or cyberattack.
4. **Ethical Issues**
    - Privacy of customer/employee data, appropriate use of financial information, and preventing misuse of system access for personal gain.
5. **Regulatory Compliance**
    - Data protection laws (e.g., Kenya's Data Protection Act) impose legal obligations on how financial and personal data is stored and processed.
6. **Why This Matters**
    - A security breach in an AIS can lead to financial loss, legal liability, and severe reputational damage - making security a core design requirement, not an afterthought.