Shamiera Stokes

Governance Memo

11/30/2025

Maintaining strong data integrity and security is essential for any information system, especially one that handles operational, organizational, or potentially sensitive user information. This governance memo outlines the policies, safeguards, and future considerations used to ensure that our MIS Helpdesk system remains secure, reliable, and fully compliant with modern privacy and security standards. The goal is to establish a clear framework for how data is protected, who has access to it, how activity is monitored, and how the system will continue evolving to meet emerging regulatory and technological changes

Protecting sensitive information is the foundation of our governance approach. Our system uses advanced encryption protocols both at rest and in transit to ensure that all stored and transmitted data remains secure and unreadable to unauthorized parties. This includes encrypted databases, secure communication channels, and strict handling procedures for any personal or identifying data. Additionally, data anonymization techniques are implemented whenever possible, especially in analytics, exported reports, and internal testing. This reduces risk if information is accidentally exposed or accessed without authorization. All privacy measures are aligned with major regulatory frameworks such as GDPR, CCPA, and other relevant compliance requirements. These frameworks guide how user data is collected, stored, and processed, reinforcing the principle that users must remain protected at all times.

Role-Based Access Control is a critical safeguard in our system. RBAC ensures that each user is granted only the permissions necessary to perform their specific duties. By assigning clearly defined roles—such as administrator, manager, analyst, or technician—we limit the possibility of unauthorized access or unintentional data exposure. This principle of least privilege not only improves security but also helps maintain an organized workflow within the system. To keep access controls accurate, regular audits are conducted. These audits verify that users still require the permissions they have and remove outdated roles or unneeded privileges. Consistent RBAC reviews reduce vulnerabilities and reinforce accountability across all system users.

Ensuring data accuracy, availability, and reliability is also central to system governance. Daily backups are performed automatically and stored in secure, redundant locations to prevent data loss from hardware failures, software errors, or unexpected incidents. Each backup is encrypted and protected using the same security protocols applied to the main system database. In addition to routine backups, scheduled restoration tests are performed to confirm that data can be recovered efficiently when needed. This process validates both the reliability of our backups and the resilience of our recovery plan. By maintaining a strong backup strategy, the system remains dependable even during disruptions and supports consistent continuity of operations.

To reinforce transparency and system oversight, an audit trail is maintained for all user actions. This includes login activity, access attempts, data modifications, administrative changes, and any other system-level interactions. The audit trail serves several important functions: it allows administrators to track unusual behavior, identify security risks, investigate potential incidents, and ensure that internal procedures are being followed correctly. In the event of an issue—such as unauthorized data access, accidental edits, or system misuse—the audit logs provide a reliable

record that allows problems to be traced back to their source. This contributes to a secure, accountable environment that discourages misuse and promotes trust.

Because technology, threats, and regulations evolve, system governance must remain adaptable. As we continue to enhance the MIS HelpDesk platform, policies will be reviewed regularly to ensure compliance with the latest standards and legislation. Future improvements may include incorporating AI-driven threat detection, expanding the use of automation in backups and audits, and integrating new privacy features as required by updated laws. This forward-thinking approach ensures that the system remains aligned with best practices and prepared for long-term operational needs.