Raise for Development and Humanitarian Aid (RDHA)

Duties Segregation System

To ensure adequate Segregation of Duties within RDHA using the proposed file management system, this can be achieved through several key features mentioned in the document:

1. **Granular Permissions Management:** This feature is foundational to enforcing segregation of duties by precisely controlling who can do what within the system.

    a. **Role Definition:** The system allows for the clear definition of distinct user roles, such as Administrator, Manager, Employee, and External User. Each of these roles is assigned a specific, predefined set of allowed permissions and actions. For instance, an "Administrator" might have full system configuration rights, while an "Employee" might only be able to upload and view documents within their department. This structured approach prevents a single user from accumulating excessive power.

    b. **File and Folder Level Permissions:** Beyond broad role-based access, the system enables the assignment of precise permissions (e.g., read-only, edit, delete, approve, publish) at a very granular level – down to individual folders or even specific files. This ensures that users can only access or modify files that fall strictly within the scope of their designated responsibilities, even if they share a common role with others in different departments. For example, a finance employee might have edit access to budget documents but only read-only access to HR policies.

    c. **Hierarchical Permissions:** Permissions can be inherited from parent folders to sub-folders. This simplifies the management of complex permission structures. While simplifying, it still maintains a clear distinction between access levels. For example, if a department head has full control over their main department folder, all sub-folders and files within it will automatically inherit those permissions, unless specifically overridden for a particular sub-folder or file to enforce a stricter segregation.

2. **Automated Workflow:** Automated workflows are critical for enforcing a sequence of actions and approvals, ensuring that no single individual can complete a sensitive process end-to-end without independent verification or action from another party.

    a. **Approval Paths:** Custom workflows can be designed to mandate approval from multiple parties or different roles to complete a specific process. For instance, a critical document might need to be initially created by an employee, then reviewed and approved by a department manager, and finally given a higher-level sign-off by a director or compliance officer. This clearly separates the duties of creation, review, and final approval, preventing fraud or errors by requiring multiple checks.

    b. **Conditional Logic:** The system can incorporate conditional logic within workflows. This means that documents can be automatically routed based on their content, metadata, or other predefined criteria. For example, a purchase request exceeding a certain monetary value might automatically be routed for an additional layer of approval from the finance department, even if a manager has already approved it. This ensures that sensitive documents pass through more stringent approval paths involving specific, independent roles.

3. **Access Auditing and Activity Log:** This feature provides transparency and accountability, acting as a deterrent against unauthorized actions and a tool for post-incident analysis.

    a. **Accountability:** The system meticulously records all activities performed on files, including who accessed, modified, deleted, or shared a file, and precisely when these actions occurred. This comprehensive log provides a complete and immutable audit trail. This trail is invaluable for ensuring accountability, as it can pinpoint the exact user responsible for any action, and helps in identifying any potential violations of segregation of duties.

b. **Monitoring:** Administrators can regularly review these detailed logs. This proactive monitoring allows them to verify that users are adhering strictly to their defined permissions and that there is no unauthorized overlap in duties. Anomalous activities or attempts to access restricted areas can be quickly identified and addressed, reinforcing the integrity of the segregation of duties policies.

4. **Authentication and Authorization:** These are the gatekeepers of the system, ensuring that only legitimate users can enter and that their permissions are correctly applied.

    a. **Strong Authentication:** The system supports and encourages strong authentication mechanisms, such as Multi-Factor Authentication (MFA). MFA requires users to provide two or more verification factors to gain access, significantly reducing the risk of unauthorized access even if a password is compromised. This is crucial because unauthorized access could bypass or compromise the established segregation of duties.

    b. **Integration with Identity Systems:** Seamless integration with established identity management systems like Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) ensures centralized management of user identities and their associated permissions. This streamlines user provisioning and de-provisioning, reduces administrative overhead, and enhances overall access control by ensuring that user privileges are consistently managed across the organization's IT infrastructure.