TRAC2 5.2.3

5.2.3 - The repository staff shall have delineated roles, responsibilities, and authorizations related to implementing changes within the system.

Explanation

SP grants authorizations and administers access controls with the intention of maintaining a high level of security and stability. As described in the repository's Security Plan, SP authorizes each staff member with limited access to system functionality based on his or her assigned duties. The Roles and Responsibilities document provides a general outline of the relationship between staff roles and specific duties. Additional controls include the following practices:

- There is no root access to critical processes, servers, or the storage array under normal circumstances. Systems administrators have root access under exceptional circumstances.
- Staff cannot write to ejournals volumes that have been mounted with a 'read-only' restriction. All ejournals volumes are mounted 'read-only' when they reach 2TB in size.
- Only systems administrators can write changes to the production servers or file system. Software developers have access to isolated development environments and the repository's code versioning system.
- SP's standard method of repairing errors in files or metadata is to request a corrected version of the article from the original Provider and re-ingest the complete package.
- Only systems administrators have access to the server room. Only the University of Toronto Libraries' Information Technology Services department can grant authorization to enter the server room.
- Only systems administrators can make changes to access controls.

Responsibility

Systems Administrator

Digital Preservation Policy Librarian

Relevant Documents

1. Security Plan
2. SP Roles and Responsibilities