International Journal of Computer Engineering & Technology (IJCET)
Volume 8, Issue 1, January- February 2017, pp. 01–04, Article ID: IJCET_08_01_001
Available online at
http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=8&IType=1
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

PLM (PRODUCT LIFECYCLE MANAGEMENT) SYSTEM ADMINISTRATOR PROCESS FOR DOCUMENT MANAGEMENT SYSTEM (DMS) IN ENERGY DEVICES DOMAIN

Ilayaraja Muthalagu
B.Sc (Computer Science), M.Sc (Information Technology), MS (Information Systems)
Senior PLM System Architect, USA

ABSTRACT

PLM System Administrator is responsible to develop a process and document that process to manage document system for energy devices such as Lithium-ion battery, Lead Acid Battery, renewable energy and green energy. This research proposal includes following PLM System Administrator processes such as procedures, policies, system configuration, document storage, system unavailability, recovery and verification, security setup. PLM System administrator must ensure all routine processes complete on schedule including the DMS system usage, maintain battery formations, routing of documents for storage, security, manage system architecture and file restoration. Process and documentation provides information to customers or team so they need to bother System Administrator less often and so saves them time. It helps PLM SAs repeat processes without any issues and simplify processes which easily be delegated to someone or team.

Key words: PLM, Product Lifecycle Management, Product Data Management, PDM, Document Management System, DMS, Energy Systems, System Admin, NPDI, Computer, Information Systems.

Cite this Article: Ilayaraja Muthalagu, PLM (Product Lifecycle Management) System Administrator Process for Document Management System (DMS) in Energy Devices Domain. *International Journal of Computer Engineering & Technology*, 8(1), 2017, pp. 01–04.
http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=8&IType=1

1. PLANNING FOR BACKUP DISASTER RECOVERY

SA develops a plan and process for backup disaster recovery. System unavailability and recovery notification process described below explains how the System Custodian and System Owner approve a disaster declaration and how key contact and users will be notified. Notification may be via phone, voice mail, email, fax, or face-to-face communication. If the system is down as the result of a server failure, an emergency is considered to have occurred when the system will be down for more than 15 hours. In the case of a fire or natural disaster, an emergency is considered to have occurred if the system will be down for more than 10 days. In the event of an emergency, the recovery team will take action as indicated. The System Custodian or System Owner declares a disaster.

2. BACKING-UP A DMS

SA documents the instructions to backing-up a DMS application. Backing up a DMS makes a copy of a DMS, which can be used to restore the DMS if it is lost. Backing up a DMS copies everything in the DMS, including any needed portions of the transaction log. The transaction log is a serial record of all the modifications that have occurred in a DMS, and which transaction performed each modification. The transaction log is used during recovery operations to roll forward completed transactions, and roll back (undo) uncompleted transactions. Backing up a transaction log backs up only the changes that have occurred in the transaction log since the transaction log was last backed up. A backup operates like a fuzzy snapshot taken of a DMS or transaction log such as a DMS backup records the complete state of the data in the DMS at the time the backup operation completes, a transaction log backup records the state of the transaction log at the time the backup operation starts. To create a sequence of transaction log backups, team typically make a DMS backup at periodic intervals, such as daily, and transaction log backups at shorter intervals, such as hourly. The interval between backups varies with the criticality of the data and the workload of the server. The sequence of transaction log backups is independent of the DMS backups. Team make one sequence of transaction log backups, and then makes periodic DMS backups that are used to start a restore operation. Disk drives provide the fastest way to back up and restore files. With disk drives, team can often accomplish in minutes what takes a tape drive hours. So when business needs mandate a speedy recovery.

3. RESTORING A DMS

Restoring a DMS backup returns the DMS to the same state it was in when the backup was created. Any incomplete transactions in the DMS backup, (transactions that were not complete when the backup operation completed originally), are rolled back to ensure the DMS remains consistent. Restoring a transaction log backup reapplies all completed transactions that are in the transaction log to the DMS. When applying a transaction log backup, DMS reads forward through the transaction log, rolling forward all the transactions on the transaction log. When DMS reaches the end of the transaction log, it has re-created the exact state of the DMS at the time the backup operation started. The restore operation then rolls back all transactions that were incomplete when the backup operation started. Backing up a DMS does not back up full-text index data in full-text catalogs. However, if full-text indexes have been defined for tables, the metadata for the full-text index definitions are stored in the system tables in the DMS containing the full-text indexes. Therefore, the metadata for the full-text indexes are backed up when a DMS backup is created. After a DMS backup is restored, the full-text index catalogs can be re-created and repopulated.

4. SYSTEM UNAVAILABILITY, RECOVERY AND VERIFICATION

If the system becomes unavailable, the following steps should be followed to ensure communication to the appropriate persons such as system owner or system admin contacts the lead data steward, lead data steward contact the support center, L2 support analyst, key business stakeholders, and reporting Account Manager, the L2 support analyst completes the initial assessment of trouble according to the corporate IT change management standard operating procedure (SOP), initiates the required trouble ticket (s), and communicates to all users, when the system is recovered, the L2 support analyst performs disaster recovery testing per the testing instructions identified in the recovery and verification section of this document and contacts the lead data steward, the L2 support analyst completes the disaster recovery execution report and supplies information to the system custodian, the system admin reviews the disaster recovery execution report, approves it, and forwards it to the system owner, the system owner reviews the disaster recovery execution report, approves it, and forwards it to the L2 support analyst, the L2 support analyst notifies the lead data steward and communicates to all of the users when the system is available, the lead data steward notifies the key business stakeholders and the system admin (and system owner), the L2 support analyst closes the trouble ticket(s), verify the availability of the system and run a base functionality script to ensure correct operation.

5. MONITORING

A service is not complete and cannot properly be called a service unless it is being monitored for availability, problems, and performance and capacity planning mechanisms are in place. The helpdesk, or system architecture team, must be automatically alerted to problems with the service in order to start fixing them before customers experience the problems. Schedule an outage plan over the weekend and alert in time to fix it before business process starts, customers don't even need to know that anything went wrong. Likewise, the PLM SA team should monitor the service on an ongoing basis from a capacity-planning perspective. Depending on the service such as network bandwidth, server performance, transaction rates, licenses, and physical device availability. As part of any service, PLM SAs can reasonably be expected to anticipate and plan for growth. *Reference: Thomas A. Limoncelli, Christina J. Hogan, Strata R. Chalup. (Second Edition). The Practice of System and Network Administration*

6. DOCUMENT THE APPLICATION SECURITY POLICIES

SA closely works with application security team and human resource team to define a security policy. The DMS security strategy has two sets of effort. The first set is for project team support for the development lifecycle of DMS. The second set is the strategy for end user security with respect to DMS application. The security strategy as it relates to other applications in the solution will be to mirror DMS as much as possible with deviations being mitigated with the controls team. PLM SA team will develop roles based on functional team input.

7. DMS PROJECT TEAM SECURITY STRATEGY

Project teams will organize tasks by functional area and create a common composite role as much as possible and then group the roles into a master composite role groups for the Team Lead, Team Member and Project Manager. The project team composite roles will match up to the job functions by team lead, team member and project manager. To control changes, only Team Leads will have authority to create transports. Team Leads and Team Members will be able to add and release tasks under the transport. Project manager roles will be view only and will not be able to make changes. The security team will have full authorizations in development to provide emergency changes and grant authorizations as needs are justified.

8. DMS END USER SECURITY STRATEGY

The security strategy for end users is to have the functional teams identify the key transactions that will be required. The process teams will also need to identify the job roles that the transactions map to for filling out the Security Matrix. This security matrix will be the key driver for creating single roles for each transaction. Composite roles will be created for each job role and the single roles will be attached. If issues occur the functional and controls team will resolve and the technical team will modify the roles based on the specifications given.

9. CONCLUSIONS

Develop a process and document that process then store it so that it's easily used, and make it available to everyone who might need it. Documentation provides information to respective team or customers so they need to bother PLM SAs less often and so save them time. It helps PLM SAs repeat processes without any issues and simplify processes which can be delegated easily. Documenting a process is difficult. However, once PLM SA has done the hard work of creating the process, the documentation can be used by anyone. Documents should be kept in a centralized storage location so they can be shared and maintained. Documentation saves us and everyone time and leverages everyone's knowledge to make a better environment. *Reference: Thomas A. Limoncelli, Christina J. Hogan, Strata R. Chalup. (Second Edition). The Practice of System and Network Administration*

DMS application is eliminating customer paper usage. A well-designed document management system eliminates the need for paper for documents used within the company and can reduce the need to send hardcopy outside the organization. *Reference: LAWRENCE WEBBER AND MICHAEL WALLACE. Green Tech How to Plan and Implement Sustainable IT Solutions. Amacom books.*

REFERENCES

[1] John Stark, (2011) Product Lifecycle Management: 21st Century Paradigm for Product Realization (Decision Engineering) 2nd edition, Springer

[2] Heckman, J., 2008. Why Document Management: A White Paper from http://www.heckmanco.com/docs/DMWhitePaper.pdf

[3] Thomas A. Limoncelli, Christina J. Hogan, Strata R. Chalup. (Second Edition).The Practice of System and Network Administration.

[4] LAWRENCE WEBBER AND MICHAEL WALLACE. Green Tech How to Plan and Implement Sustainable IT Solutions. Amacom books.

[5] R.Sharmila and Dr.A.Subramani, Impact of Business Intelligence Tools in Executive Information Systems. *International Journal of Computer Engineering & Technology (IJCET),* 4(1), 2013, pp. 01–07

[6] http://help.sap.com/saphelp_erp2004/helpdata/en/c1/1c31a243c711d1893e0000e8323c4f/frameset.htm

[7] http://www.cimdata.com/en/

[8] Andrea Buda, Petri Makkonen, PDM suitability study for CAE data management: http://www.ifip-wg51.org/

[9] Akbar Jamshidi and Jafar Jamshidi, New Product Data and Process Management – A Case Study of PLM Implementation for Formula Student Project: : http://www.ifip-wg51.org/

[10] Frédéric Demoly*, Dimitris Kiritsis, An integrated requirements elicitation approach for the development of data management systems: http://www.ifip-wg51.org/

[11] Radhika P Arethoti, An Overview on Achieving Product Service Management in End-To-End PLM System. *International Journal of Computer Engineering & Technology (IJIERD),* 3(2), 2012, pp. 10–17.