Georgia Department of Transportation

GDOT Publications
Policies & Procedures

Policy: 8075-4- Database Systems Standard
Section: Database Standards
Office/Department: Office of IT Applications

Reports To: Division of Information Tech
Contact: 404-631-1000

PURPOSE

The purpose of this standard is to ensure database integrity, high availability, optimum performance, and effective operations. All IT development projects are required to adhere to these standards. This standard applies to enterprise class database management systems.

SCOPE

This policy applies to all GDOT IT personnel (including employees, consultants, contractors, vendors and other third parties) actively engaged in the support, deployment, or modification of any enterprise class database.

Exception to this standard must be approved by the Administrator of IT Application Support & Development.

RESPONSIBILITY

1. The Administrator of the Office of IT Application Support & Development is responsible for compliance with the standard, updates to the standard, and enforcing the standard.
2. GDOT IT Team Leaders are responsible for compliance with the standards and for reporting concerns to the IT Application Support & Development Administrator.

STANDARDS

Design Specification and Requirements

1. A high-availability, business continuity, and/or disaster recovery strategy must be implemented for databases that are essential for:
   - Performing Homeland Security or Georgia Emergency Management Authority (GEMA) Emergency Support Functions (ESF)
   - GDOT to respond effectively to an emergency situation or natural disaster
   - Performing critical operations or business functions of GDOT during a system outage
2. OLTP (Online Transaction Processing) data that is used by online users for mission-critical day-to-day operations and OLAP (Online Analytical Processing) data used for ad-hoc queries and decision support should be segregated into separate databases and/or servers.
3. All replicated and archived data must be designed to be read-only. Updates must occur at the source where the data originates to promote data integrity and facilitate ease of data management. Replication of data must be based on requirements such as availability, security, performance, or decision support. Replication shall be used to:
   - insure uninterrupted access to critical data
   - isolate production data from external users

- facilitate load balancing through synchronization of distributed databases
- facilitate performance within the IT application

4. Any new database implementation or migration of legacy data source to GDOT target data architecture shall use a GDOT approved relational DBMS, and support ANSI Standard SQL (currently SQL92), and shall also comply with ODBC and JDBC standards.
    - WE8MSWIN1252N will be the standard NLS_CHARACTERSET used. Additional character sets required for the functioning of a given application must be approved by the Office of IT Application Support & Development Administrator.
    - The use of standard features shall be favored over optional vendor-specific features to prevent being locked into a vendor-specific solution.
5. The source data that populates the Enterprise Data Warehouse (EDW) or Geographic Information System (GIS) must adhere to integrity constraints or accuracies required of the source system.
6. Any data updates to an authoritative source OLTP system will only be carried forward after being entered into the source system and all of the governing business rules have been applied. Commercial off the Shelf (COTS) software shall be configurable to allow for data validation. To reduce the risk of inaccurate or misleading data and to reduce the need for data cleansing, data quality validations shall be built into new and existing systems.
7. All systems should include an accurate data or geodata model, created by a cooperative effort between the Business Unit and IT Applications to ensure that the logical and physical designs satisfy the business requirements.
8. Archive and/or purge criteria shall be established for all databases. Data that is no longer needed shall be purged or archived to a less expensive media in accordance with GDOT data retention requirements, policies, or historical significance.
9. Metadata with its security classification shall be captured and maintained for both OLTP and OLAP environments to facilitate data sharing within GDOT and among its business partners. Business process owners and developers, including contractors, are responsible for documenting elements stored in the database, and shall follow the GDOT metadata standards.

Production Specifications and Requirements

1. When implementing a data warehouse or data mart, an assessment shall be done to determine the potential impact on the network and to assess the historical and/or analytical value of the data.
2. Microsoft Access databases and other desktop or non-approved databases shall not be used to develop standalone applications. Microsoft Access shall not be used to support enterprise reporting. These types of systems are difficult to support and shall not be used to support critical business functions. Furthermore, Microsoft Access databases and/or applications will not be supported or developed by the Office of IT Application Support & Development.
3. Production databases supporting mission-critical applications must be recoverable to a point-in-time and point-of-failure.
    - Database transaction logging must always be active for mission-critical production applications. Database backups must be sent offsite weekly, at a minimum.
    - A backup/recovery plan must be in place and tested at least twice a year to prevent loss of data due to application/software errors, or from hardware failures.
    - Database backups shall be scheduled frequently enough to ensure optimum recovery times.
4. An internal auditing process shall be put in place to ensure that GDOT is in compliance with all security, privacy, and information dissemination laws. Database Administrators should work closely with security officers to ensure that information is stored, managed, accessed and secured in compliance with Federal and State privacy laws as well as other laws impacting GDOT program areas.
5. All platforms used for hosting mission-critical applications shall be fully supported by the vendor and provide optimum performance. DBMS vendors acknowledge these platforms as preferred or tier-1. Vendor support shall provide better

access to the latest versions of products, timely patches, and to knowledgeable technical support on preferred/tier-1 platforms.

6. For new database development efforts, Business Continuity (BC) or high availability architecture requirements will be addressed in the Architecture Design. A Disaster Recovery (DR) Plan shall be created that documents the operational procedures required for the recovery, including procedures for retrieving offsite copies of database backups. The EDW Team Leader and the Database Support & Development Team Leader shall ensure that all DBA's understand the steps needed to perform a recovery, validate data integrity, and minimize downtime. Documented DR plans will be used for DBA's to perform drills/readiness exercises.
7. Databases for mission-critical applications shall be monitored proactively for capacity planning purposes and to maintain high availability. Statistics such as transaction rates, allocated extent size, system CPU, and archive log volume shall be included. A database should not stop functioning for foreseeable events. Events such as file systems filling up, objects not able to allocate additional extents, and objects reaching max extents shall be actively monitored and a DBA notified, before the problem causes the database to halt.
8. Database permissions shall be granted at the minimum level required.
    a. Limit the members of the System or Database Administrators role to trusted DBAs.
    b. Create custom database roles, if required, for better control over permissions.
    c. Application programs or interfaces shall never be given "sysadmin" / "sysdba" / "sde" authority.
    d. Default accounts shall be changed.
    e. Production passwords shall be changed from test or development environments.
    f. A process shall be put in place to periodically re-assess access.
9. Error logs and event logs for security-related alerts/errors shall be monitored, and notifications shall be sent to database administrators for appropriate support task. The use of Intrusion Detection Systems (IDS), especially on mission-critical database servers, must be implemented. IDS can constantly analyze the inbound network traffic, look for trends and detect Denial-of-Service (DoS) attacks and port scans. IDS can be configured to alert the administrators upon detecting a particular trend.
10. DBAs shall remain current with the information on the latest service packs and security patches released by DBMS vendors. All the service packs and patches shall be carefully evaluated and applied according to the DBMS vendor recommendations.
11. Capacity planning shall be performed bi-annually or with system upgrades to assess or forecast future storage/hardware/software requirements.
12. Databases shall be stress tested to simulate anticipated normal and peak usage of the system.
13. Statistics related to normal database operations, networks and applications shall be collected and available for a minimum of 3 months.
14. A change management process to coordinate and communicate infrastructure, application, and database related changes shall be put in place.
15. Database Management Systems and the Operating System versions/patch levels shall be compatible, and vendor supported.

References:

None.

History:

annual review: 06/14/23;
new policy effective 09/01/09: 10/01/09;