BUREAU OF UNDERWATER RESOURCES AND PETROLEUM SERVICES

DATABASE POLICY STATEMENT

It is the purpose of this policy statement to insure that BURP's data base policies are in line with the best practices in the industry and in compliance with all federal requirements to protect confidential information and to conform to the Federal Privacy Act.

MANAGEMENT PROCEDURES
The Bureau’s Chief Information officer will be responsible for all policy and procurement decisions. The officer will oversee all the maintenance, development and enhancement of the group’s database.

ACCESS RESTRICTIONS AND PRIVILEGE
The CIO and his team will be responsible for developing three levels of user access. Level 1 access will be granted to those individuals whose job responsibilities require them to have access to the data and database. Level 2 Access will be granted to those individuals who require entering and changing data in the database. Individuals given Level 2 Access will be required to successfully complete one ½ day tech training session and their access will need to be approved by the CIO. Level 3 Access professionals will be those individuals who have access not only to the data but also to reach code in the relationship tables. Access will be assigned only to 3 senior members of the CIO team.

SECURITY AND FIREWALL
Security and Firewall construction issues are among the most important aspects of the data environment in which we operate. The CIO Office will have a single officer, the bureau’s IT Security Office (ITSO). Together with the CIO, the ITSO will be responsible for guaranteeing that the bureaus system is compliant with current federal standards and is not vulnerable to hacking from the outside.

CHANGES AND RECOVERY
The bureau is all required to ensure all data is properly backed-up in the case of a disaster/ emergency. Subject to Bureau head and CIO approval, the data backup may take place via cloud computing solutions (such as Oracle) or external hard drives.

PASSWORD SECURITY
All users must have passwords that are at least 16 letters and include two numeric keys and one symbol. Passwords may not be shared or divulged to any user. Additionally, they must be changed every six months.

BUSINESS CONTINUITY PLANS
The bureau is required to participate in an offsite business continuity plan. The group will need to ensure external backup data can be accessed away from central database and that key employees will have the required infrastructure to work from the business continuity site in case of emergency.

MAINTENANCE, AUDIT AND UPGRADE
A regularly scheduled maintenance will be conducted annually. A team of individuals with Access Level 3 clearance as well as the CIO will approve all upgrades.

EXTERNAL SOFTWARE
No external software may be downloaded to any of the computers in this bureau. The level 3-access team shall approve any new software being implemented.