PERMANENT MEMORANDUM 36
ATTACHMENT 2 – GLOSSARY

Business Associate Contract Addendum - See Attached

Business Continuity Plan (BCP): plan and preparations directed towards either the immediate recovery of systems critical to the function of the business, or to the ability of the business to operate in the temporary absence of important systems

Digital Communication: electronic exchange of information (e.g., e-mail, cellular phones, instant messaging)

Disaster Recovery Plan (DRP): a plan and preparations directed towards the resumption of business and the recovery of systems after catastrophic loss of important systems. A disaster recovery plan is generally concerned with longer time frames than a business continuity plan. Sometimes also referred to as a business resumption plan.

Louisiana Office of Information Technology (OIT): Provides the electronic government structure for the executive branch of state government as directed by ACT 772 -2001 Regular Session http://www.legis.state.la.us/bills/byinst.asp?sessionid=01RS&billtype=SB&billno=455

National Industrial Security Program Operations Manual (DOD standard 5220.22M): This manual is issued in accordance with the National Industrial Security program (NISP). The Manual prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. The Manual also prescribes requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including *restricted data, formerly restricted data, intelligence sources and methods information, sensitive compartmented Information, and Special Access Program information.* These procedures are applicable to licenses, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations. http://www.dss.mil/isec/nispom_0195.htm

Owner of Information Systems: Internal and permanent staff member with the competence required to evaluate and classify a certain number of systems for which he is accountable. Information system owners grant access rights to the information systems they own and ensure that adequate security measures are taken to protect this information, and to guarantee its integrity and confidentiality. Even though the overall responsibility falls entirely to information system owners, they have the power to delegate certain tasks to employees under their direction.

Parallel Running: The process of running a new or amended system simultaneously with the old system to confirm that it functions correctly before going live.

Protected or Restricted Information: information that shall have extraordinary controls over its use and disclosure due to the sensitivity of its content. Examples of Protected information include, but are not limited to: employment records, medical records, student records, personal financial records (or other

individually identifiable information), research data, trade secret information and classified government information. Restricted information is information of such a sensitive nature that access is limited to those individuals designated by management as having a need to know. Examples of restricted information include, but are not limited to ongoing investigations, pending litigation, psychology notes and disciplinary action.

Segregation of Duties: a method of working where tasks are assigned to different members of staff to reduce the occurrence of error or fraud.

Server Rooms: rooms that contain computers/devices which provide information or services to computers on a network.

Attachment: Business Associate Contract Addendum