Q. DISASTER RECOVERY/BUSINESS CONTINUITY

OBJECTIVE

The Disaster Recovery/Business Continuity Policy aims to coordinate the recovery of critical business functions in managing and supporting the business recovery in the event of a disruption or disaster, including all computer systems and networks. This can include short or long-term disasters or other disruptions, such as cyberattacks, fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters.

A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization's ability to deliver essential business services.

This policy is intended to remain dynamic. Typically, the Greater Lafourche Port Commission will review this policy at least annually and, if deemed advisable, recommend changes.

IDENTIFICATION OF CRITICAL DATA AND FREQUENCY OF DATA BACKUPS

The Greater Lafourche Port Commission, Director of Information Technology, must work with all department heads annually to review which systems are most critical to the organization. This list will be prioritized by the Director of Information Technology and brought to the Executive Director for approval. This can be done through a formal data classification process or an informal review of information assets. Regardless of the method, critical data must be identified to be given the highest priority during the backup process.

Backups of critical systems are done hourly within the data center, daily to a cloud repository. monthly to tape.

The list of critical data can be found in the Director of Information Technologies safe located in server room of the GLPC Administrative Office at 16829 East Main St., Cut Off, LA 70345

STORAGE OF BACKUPS IN A SEPARATE PHYSICAL LOCATION ISOLATED FROM THE NETWORK

Backups tapes are taken off-site at least once per month. Detailed information about the separate physical location isolated from the network can be found in the Director of Information Technologies safe located in server room of the GLPC Administrative Office at 16829 East Main St., Cut Off, LA 70345

PERIODIC TESTING/VERIFICATION THAT BACKUPS CAN BE RESTORED

Backup restores are tested at least once every three months. Detailed information about testing/verification can be found in the Director of Information Technologies safe located in server room of the GLPC Administrative Office at 16829 East Main St., Cut Off, LA 70345

USE OF ANTIVIRUS SOFTWARE ON ALL SYSTEMS

All GLPC computers and servers are protected by antivirus software. The details of the Antivirus Software can be found in the Antivirus Management Console.

TIMELY APPLICATION OF ALL AVAILABLE SYSTEM AND SOFTWARE PATCHES/UPDATES

All computers, servers, and network devices must be maintained at vendor-supported levels, and critical security patches must be applied in a timely manner consistent with an assessment of risk performed by the GLPC IT Department.

GLPC IT Department will review, evaluate, and appropriately apply software patches in a timely manner. If patches cannot be applied in a timely manner due to hardware or software constraints, mitigating controls will be implemented based on the risk assessment results.

Details on the process can be found in the Patch Management Console.

IDENTIFICATION OF PERSONNEL, PROCESSES, AND TOOLS NEEDED TO RECOVER OPERATIONS AFTER A CRITICAL EVENT

The GLPC IT Department is responsible for managing disaster recovery efforts. The recovery is activated at the call of the Executive Director when a disaster occurs. The details of the processes and tools needed to recover operations after a critical event can be found in the Director of Information Technologies safe located in server room of the GLPC Administrative Office at 16829 East Main St., Cut Off, LA 70345

RESPONSIBILITY

The Director of Information Technology is responsible for auditing information systems to ensure they comply with this policy.