Q. DISASTER RECOVERY/BUSINESS CONTINUITY

OBJECTIVE

The objective of the Disaster Recovery/Business Continuity Policy is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a facilities (Port office building) disruption or disaster which would include 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 not intended to remain static. Normally, 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 Homeland Security and Technology ("The Director") 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 and then brought to the Executive Director for approval. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data must be identified so that it can be given the highest priority during the backup process.

Backups of critical systems are done hourly and stored at an offsite facility. Full replication of critical systems is done every 60 (sixty) minutes to an offsite facility. Testing of replication to offsite facility is conducted annually.

The list of critical data and the detailed information about the offsite facility can be found in the GLPC Information Technology Disaster Recovery and Business Continuity Plan upon request as this is considered Sensitive Security Information (SSI).

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

Backups tapes are taken off-site at least once per month. The detailed information about the separate physical location, which is isolated from the network, is considered SSI and can be found in the GLPC Information Technology Disaster Recovery and Business Continuity Plan.

PERIODIC TESTING/VERIFICATION THAT BACKUPS CAN BE RESTORED

Backup restores are tested at least once every 6 months. The detailed information about the testing is considered SSI and can be found in the GLPC Information Technology Disaster Recovery and Business Continuity Plan.

USE OF ANTIVIRUS SOFTWARE ON ALL SYSTEMS

All GLPC computers and file servers are protected by antivirus software. The details of the Antivirus Software are considered SSI and can be found in the GLPC Cybersecurity Strategic Implementation Plan.

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 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 upon the results of a risk assessment.

Details on the process are considered SSI and can be found in the GLPC Cybersecurity Strategic Implementation Plan.

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 are considered SSI and can be found in the GLPC Information Technology Disaster Recovery and Business Continuity Plan.

RESPONSIBILITY

The Director of Homeland Security and Technology is responsible for auditing information systems to ensure they comply with this policy, the GLPC Information Technology Disaster Recovery and Business Continuity Plan, and the GLPC Cybersecurity Strategic Implementation Plan.