Operation/Task:	Backup Restore Disaster Recovery			Equipment:	N/A
Owner:	Vice President of Technology	Date Prepared:	12/15/14	Department Responsibilities:	IT Support Team
		Revision History:	See last page		

ALERTS (see below):   Critical Step ◆   Quality Check ☑   Tip ☺   Team Safety ✚

Purpose: This SOP/work instruction purpose documents procedures to ensure accuracy in Ecommerce orders, customer requests and to make sure that IT staff is responding timely and appropriately to user requests.

Step #	Alerts	Step Description - "What to Do"	"How to Do it"	"Why to Do it"
1	☑	Backup and Restore	Backup processes exist for all business defined critical information including financial, database, email, graphics, and operating system files. Full backups will occur on the weekends and incremental backups will occur daily during the week. Backups are kept for 30 days. Backup files will be written to a disk repository storage system. Daily backup log reports are sent to IT Support distribution list. Including list of content and current location. The backup system maintains inventory records for all backups, including content, date/time, source location, and destination location. IT Support will restore the file(s) from the appropriate disk repository storage system upon request from the IT ticketing system.	The restoration of files from backup repositories occurs because of file or database corruption, server failure or inadvertent deletion of data.

| 2 | ☑ | Disaster Recovery | The company Disaster Recovery Plan refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. The high-level recovery plan includes one or more approaches to restore disrupted IT services.
- Restoring IT operations at an alternate location
- Recovering IT operations using alternate equipment
- Performing some or all of the affected business processes using non-IT (manual) means until automated business processes can be restored
In a disaster recovery scenario, Key Personnel would determine the extent of damage and determine the correct backup files to restore at the appropriate location. In addition, appropriate vendors would be contacted and the equipment would be delivered and installed at the alternate location. The Executive team would determine when operations would return to the original location. | Due to the company's dependency on information technology to run operations, a disaster recovery plan is necessary to recover operations if the data, assets, and facilities become damaged. |

Notes:

Definitions:

Revision History	Description of Changes	Requested by	Date
Rev 1	Revised SOP to new format	Jon Peters	12/15/14
Rev 2	Added Revision History table	Jon Peters	8/1/16
Rev 3	Reviewed and change ITNS to IT Support, changed gray header date information, changed operation/task name	Jon Peters	4/13/20
Rev 4	Replaced additional references to IT Network Services with IT Support. Replaced IT Compliance and Security Manager with IT Systems Manager Revised header, font type, and font size to be consistent with other SOPs Removed references to GLS	Mike Starrett	12/30/20
Rev 5	Removed ref to Exchange backups and changed wording on backup notifications going to IT Support Team	Eric Crichton	12/12/2022
Rev 6	Reviewed by Eric Crichton, no changes made		8/30/23

| Rev 7 | Replaced IT Systems Manager owner with Vice President of Technology | Mike Starrett | 11/4/2024 |

CI035 4/20