SOP # ______ Revision:______ Prepared by:____________

Effective Date:______________ Approved by:____________

Title: ITSD104 – IT DISASTER RECOVERY

Policy: To ensure continuity of Company operations.

Purpose: To define recovery objectives and to specify a set of procedures for achieving those objectives.

Scope: This policy applies to all Company personnel and IT systems, networks, and assets.

Responsibilities:

The IT Disaster Recovery Coordinator (IT DRC) is responsible for chairing the IT Disaster Recovery Planning Committee, coordinating IT disaster response and recovery, reporting on disaster response and recovery, and updating the Recovery Plan.

The IT Security Manager is responsible for conducting and/or supervising testing of the IT Disaster Recovery Plan.

The IT Disaster Recovery Planning Committee (IT DRPC, or "the Committee") is responsible for developing and reviewing the IT Disaster Recovery Plan.

The IT Storage Librarian is responsible for backing up and restoring Company data.

Tech Support staff are responsible for various recovery tasks, such as installation and testing of replacement equipment, operations systems, applications software, communications, etc.

Top Company Management is responsible for final approval of the IT Disaster Recovery Plan.

All Company employees are responsible for notifying the IT DRC in the event of an actual or suspected disaster that may affect any part of the Company's IT systems, infrastructure, or assets.

Definitions: Business continuity – The degree to which an organization may achieve uninterrupted stability of systems and operational procedures.

IT disaster – A sudden, significant event that may result in the loss or destruction of Company information and/or loss of service on the Company's IT network.

Procedure:

1.0 IT DISASTER RECOVERY PLANNING

1.1 The Company must assume a major disaster – environmental disaster, loss of utilities, large-scale equipment failure, a cyberattack, and so on – will befall it eventually. To be prepared for disaster – to best ensure the continuity of business, should a disaster occur – the Company shall develop an IT Disaster Recovery Plan. The IT Disaster Recovery Plan (DRP) shall be an integral part of the Company's overall DRP, just as information technology is an integral part of the Company. (See Reference A.)

The Company shall implement the Plan, educating employees in their roles and responsibilities; test the Plan, to see if it will ensure rapid and full recovery; and fix flaws identified in testing, to better ensure the Plan will work when it is most needed.

1.2 The Company shall establish an IT Disaster Recovery Planning Committee (IT DRPC), composed of key personnel from each functional area within the Company (HR, accounting, sales, etc.) and an IT Disaster Recovery Coordinator, who shall chair the Committee.

1.3 The IT Disaster Recovery Coordinator shall obtain and analyze information for development of the IT Disaster Recovery Plan, such as:

- Conducting a risk assessment of each of the Company's IT systems, in accordance with ITSD101 – IT THREAT/RISK ASSESSMENT;
- Determining the IT Department's current state of readiness for disaster by running a recovery capability test, to establish a baseline;
- Gathering IT industry information on best practices and technologies and identifying appropriate means of mitigating risk; and
- Identifying and assessing external resources and their capabilities.

1.4 The IT DRPC shall meet to:

- Analyze and discuss the information obtained by the IT Disaster Recovery Coordinator:
- Identify mission-critical systems and services, determining how long each business unit can survive without those systems/services in operation (conduct a business impact analysis);
- Establish recovery priorities;
- Develop the IT Disaster Recovery Plan in accordance with ITSD102 – IT SECURITY PLAN, using ITSD104-1 – IT DISASTER RECOVERY PLAN as a guide.
- Submit to top management for final approval.

1.5 The IT Disaster Recovery Coordinator shall:

- Ensure that the IT Disaster Recovery Plan is documented and communicated to all Company employees; and
- Coordinate IT disaster recovery training with the Human Resources Manager.

2.0 IT DISASTER RECOVERY PLAN

2.1 The IT Storage Librarian shall ensure periodic backups of Company information stores (databases, etc.), in accordance with ITSD103 – IT MEDIA STORAGE.

2.2 The IT Storage Librarian shall periodically conduct a test of all backed-up data for integrity and recovery speed; frequency and extent of such testing shall be determined by mission criticality of the information. The Storage Librarian shall submit a recovery test report to the IT Disaster Recovery Coordinator for review and possible action.

2.3 In the event any employee knows of or suspects an IT disaster, the employee shall contact the IT DRC and the DRC shall begin the response and recovery process in accordance with the Plan.

3.0 IT DISASTER RECOVERY PLAN REVIEW

3.1 Subsequent to an actual disaster and recovery, the IT Disaster Recovery Coordinator shall prepare a response and recovery report and submit it to the IT Disaster Recovery Planning Committee for review. The Committee may recommend revisions to the Plan, based on the findings contained in the report.

3.2 The IT Security Manager shall test IT disaster response and recovery at least once every 12 months. The IT Security Manager should also test response and recovery upon any changes to the Plan (see section 4.2).

3.3 The IT DRPC shall review the IT Disaster Recovery Plan on a regular basis (every two years, at a minimum) to determine if it continues to meet Company, customer, and legal/regulatory requirements.

3.4 The IT Disaster Recovery Plan shall be periodically (at least once every three years) subjected to a third-party audit, to verify that the Plan is clear, sound, and continues to meet Company, customer, and legal/regulatory requirements.

4.0 IT DISASTER RECOVERY PLAN REVISION

4.1 After any review of the IT Disaster Recovery Plan, the IT Disaster Recovery Coordinator shall be responsible for updating the Plan.

4.2 Within one month of any such update, the IT Security Manager shall verify that the update is capable of providing the desired results by conducting a response and recovery test.

Additional Resources:

A. The Business Software Alliance (BSA - http://www.bsa.org/) is, according to its website, the foremost organization dedicated to promoting a safe and legal digital world. BSA calls itself the voice of the world's commercial software industry and its hardware partners before governments and the international marketplace.

B. The CIO Executive Council is a professional organization for chief information officers. It can be a valuable source of information for disaster recovery planning. See http://www.cioexecutivecouncil.com for information.

C. Schreider, Tari, "The Legal Issues Of Disaster Recovery Planning", Disaster Recovery Journal, April-June, 1996. See http://www.drj.com/new2dr/model/schr.htm.

D. The International Association of Emergency Managers (IAEM) is a non-profit educational organization dedicated to promoting the goals of saving lives and protecting property during emergencies and disasters. For more information, go to http://www.iaem.com/.

E. The Disaster Recovery Journal web site (especially the "Tools" group of links) is extremely helpful. The address of that web site is http://www.drj.com/.

References:

A. BIZMANUALZ PUBLICATION #ABR33M - DISASTER RECOVERY POLICIES, PROCEDURES, AND FORMS

This publication is a prototype, or template, for developing a physical disaster recovery plan suited to an organization's needs and requirements. Any IT disaster recovery plan must be integrated into the organization's overall DRP, because IT is an integral part of any organization and because IT disasters may have a physical dimension to them. Fire and flood, for example, have the potential to cause serious harm to life and property and disrupt IT operations.

B. THE PUBLIC COMPANY ACCOUNTING REFORM AND INVESTOR PROTECTION ACT OF 2002 (SARBANES-OXLEY, SOX)

While Sarbanes-Oxley (US law) does not specifically mention "disaster recovery", universal acceptance and use of information technologies and the requirements of SOX – that a public company demonstrate "adequate internal controls" and ensure integrity and timeliness of its financial records - imply that a disaster recovery plan is needed for an organization to maintain compliance with SOX.

C. ISO/IEC STANDARD 17799:2005 – INFORMATION TECHNOLOGY- CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, CLAUSE 8.4.1 (INFORMATION BACK-UP)

Clause 8.4.1 contains minimum standards and controls for backup and restoration of Company data, such as storing essential data in a remote site, protecting backup information, testing backup data, and checking restoration procedures regularly.

D. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

HIPAA (US law) is designed primarily to allow patients access to their medical records and ensure privacy and portability of those records. The Act requires health care providers to have a "reasonable and appropriate" data backup plan, disaster recovery plan, and plan for operating in emergency mode.

E. EXPEDITED FUNDS AVAILABILITY ACT OF 1989 (EFA)

The EFA Act (U.S. law) requires that federally chartered financial institutions have a "business continuity plan" to ensure prompt availability of funds.

F. NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION #800-53 – RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS (FEBRUARY, 2005)

This publication refers to contingency plan development, testing, update, and coordination. See http://csrc.nist.gov/ for details.

G. FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA) PUBLICATION #141 – EMERGENCY MANAGEMENT GUIDE FOR BUSINESS AND INDUSTRY (OCTOBER, 1993)

Despite its apparent lack of success in 2005 with Hurricanes Katrina and Rita, FEMA has developed an excellent guide that can help businesses develop their own disaster recovery plans (DRP). This file, in PDF format, may be found at: http://www.fema.gov/pdf/library/bizindst.pdf.

Revision History:

Revision	Date	Description of changes	Requested By
0	6/11/2008	Initial Release	