X-ISS *Delivering eXcellence in IS Solutions since 1993*

www.x-iss.com

How well is your IT prepared for a disaster or outage?

The primary objective of disaster recovery planning is to protect the organization in the event that all or part of its operations and/or computer services are rendered unusable. Preparedness is the key.

A good Disaster Recovery Plan:

- ❖ Minimizes potential economic loss.
- ❖ Reduces disruptions to operations.
- ❖ Minimizes insurance premiums.
- ❖ Minimizes decision-making during a disastrous event.
- ❖ Provides peace of mind.
- ❖ Reduces reliance on certain key individuals being present to implement it.
- ❖ Minimizes risks of recovery delays and provides for an orderly recovery.
- ❖ Protects the assets of the organization.
- ❖ Ensures the reliability of back-up systems.

THE X-ISS 18-POINT DISASTER RECOVERY PLANNING CHECKLIST

Disaster recovery planning involves more than off-site storage or backup processing. To be best protected and prepared in the event of an outage or disaster, each business needs a written, comprehensive disaster recovery plan that addresses all of the critical operations and functions of their business. Here are some of the key elements of an effective Disaster Recovery Plan to help you further assess or develop your plan:

___________ **Management support:** The essential element for the success of any Disaster Recovery Plan is support from the top. The development and maintenance of the plan requires ongoing support to keep it relevant.

___________ **Risk assessment analysis:** Potential vulnerabilities and threats of the geographic location(s), security posture, hardware, software, and network design have been identified and analyzed.

___________ **Business Impact Analysis (BIA):** The organization's vital functions, impact of the outage, potential loss of revenue, essential staff, and regulatory and contractual obligations, and what is needed to allow the organization to support its critical business functions have been analyzed and documented.

___________ **Preventative controls:** The plan includes both deterrent and preventative controls which attempt to cover as many identifiable risks as possible. Some of the controls that should be reviewed can include physical security, personnel procedures, infrastructure (generators, UPS, fire suppression), software controls such as anti-virus, firewalls, intrusion detection, backup and retention processes.

____________ **Activation parameters:** The plan clearly states the parameters for when it needs to be activated. The individuals with the authority to declare a disaster and their designees are clearly defined in the plan.

____________ **System/application prioritization:** Restoration priorities are established so during a disaster energies are focused on the recovery of essential functions first.

____________ **Roles and responsibilities:** Roles and responsibilities are clearly defined, so that no ambiguity will exist about who is in charge for each task. Back-ups have been designated and processes put in place to ensure plans don't rely upon just one critical person to be present to be conducted.

____________ **Communication plan:** The plan documents who is to be informed of the outage or disaster and what will be the method and frequency of the status updates during the event. Keeping customers, employees, and all stakeholders apprised of the recovery efforts is critical during a business interruption. Alternative communication methods were considered and are incorporated, as needed, based on the type of outage.

____________ **Data/Back-up plans:** All forms of necessary data have been inventoried, and appropriate back-up schedules have been put in place. The plan documents replication schedules and storage locations. Critical data is stored minimally daily at an off-site secure location.

____________ **Staff call tree:** All staff members have a current, verified call tree with multiple contact numbers (office, home, cell, personal e-mail, close friends, or relatives). This is often a weak link during an event because normal communication channels might be affected during an outage.

____________ **Key vendors**: A current list of all vendors that might be required to provide support during and after the event is included. All vendors that can provide office supplies, PCs, and furniture depending on the event have been considered, emergency purchasing procedures have been identified.

____________ **Contract information:** Relevant contract information, such as agreements with vendors for emergency services or equipment, is included in the plan.

____________ **Other key documents/contact information:** Additional key information including emergency phone numbers, insurance policy information, etc. have been included.

____________ **Identification of alternate locations**: The plan lists alternate locations designated for systems and staff. Staff should know in advance to where they should report if their primary work location is not available.

____________ **Detailed system restorations procedures**: For each application/system that needs to be restored, detailed instructions for restoration are included. The restoration procedures are written in such a way that if the primary resources are not available, a person with basic knowledge of the platform can restore the system based on the written and exercised procedures.

____________ **Testing**: The plan has been tested in the past six months. Results and guidelines for when to perform further tests are documented in the plan.

____________ **Plan maintenance and distribution**: The plan details how it will be distributed, any necessary version differentiations and how it will be maintained.

____________ **Returning to normal:** Procedures to restore business processes and systems to their original location are provided.

How prepared are you? Do you need assistance in developing an effective, affordable disaster preparation, protection and recovery plan?

For a plan that's tailored to your business needs and budget

CALL 713.862.9200 TO SCHEDULE AN APPOINTMENT WITH AN X-ISS EXPERT TODAY.

ABOUT X-ISS: (www.X-ISS.com)

X-ISS is the trusted choice of small-to-medium businesses in the Greater Houston area who want to maximize the performance and protect the security of their IT resources affordably. Best known for their exceptional expertise and customer service, they have been creating cost-effective, business saving disaster recovery protection and preparation plans for a wide range of loyal clients for over fifteen years.

What some X-ISS clients say:

"Recently one of our architectural projects ran into predicament with an extremely important file on our server the night before a major submittal. Something that would have taken us 60+ man hours to do was easily recovered in minutes. We are extremely pleased with the X-ISS Team."

– Alex Nguyen, Studio RED Architects. Houston, TX

"X-ISS has really come to our rescue. Your assistance… has been critical to our day to day operations." **–Chroma Exploration**

"X-ISS…is a trusted consultant for … our data network" **–GX Technology**

"X-ISS delivered and continues to deliver." **– The Office of George Bush**