

The disaster recover policy must be reviewed at least annually to assure its relevance.

To ensure that the policy and the Disaster Recovery Plan is administered effectively a planning team consisting of senior management and personnel from IT, HR and other operational departments should be assembled to review the disaster policy and the plan.

Roles and Responsibilities

- The roles and responsibilities of the incident management team (IMT) should be as follows:
- Perform an initial risk assessment to determine current information systems (IS) vulnerabilities;
- Perform an initial business impact analysis to determine and understand the inter-dependencies among business processes and determine how the business would be affected by an information systems outage;
- Take an inventory of information systems assets such as computer hardware, software, applications and data;
- Identify single points of failure within the information systems infrastructure;
- Identify critical applications systems and data;
- Prioritise key business functions;

Implementation Procedure

Company personnel will carry out the following procedures in the implementation of a disaster recovery policy:

- Setup and maintain facilities for the backup and storage of electronic data as well as reliable standby systems if necessary;
- Ensure that critical application systems and data are reasonably easy to get to but far enough away not to be affected by the same disaster;
- Establish written policies, contracts and service agreements with third party hosting collocations and telecommunications and internet service providers that facilitates prompt recovery and continuity;
- Create an incident response team (IMT), that consists of information security (IT), marketing, HR, legal and other relevant personnel;
- Define the roles and responsibilities of the IMT members in a suitable document and issue;
- Obtain each IMT members contact information and develop an escalation process;
- Determine which methods the IMT members will use to communicate in the event of a disaster e.g. email, mobile phone etc;
- Create a public relations plan to assist with the effective handling of an incident;
- Assign a manager that has the responsibility and authority to make critical IT decisions;
- Develop testing standards;
- Document copies of the written plans to everyone involved specifically the IMT, and also store extra copies in an offsite fireproof vault;





Disaster Recovery Policy

- Document a reduced version of the DR Plan and communicate to all staff
- Establish an emergency telephone number and communicate the number to all staff

Testing and Review

The following ongoing procedures must be followed:

- Continuously perform data back-ups, store at least weekly back-ups off-site and test those backups regularly for data integrity and reliability;
- Test plans at least annually and document and review the results and update the plan regularly;
- Analyse the plans on an ongoing basis to ensure alignment with current business objectives and requirements;
- Provide security awareness and disaster recovery education for all team members involved;
- Continuously update information security policies and network diagrams
- Secure critical applications and data by patching known vulnerabilities with the latest fixes and or software updates;
- Perform continuous computer vulnerability assessments and audits;

Reference Documents

The following documents are to be read in conjunction with this policy

- IMT Plan
- Business Continuity Plan Guidelines
- IT Security Policies and Procedures

This statement represents our general position on DR issues and the policies and practices we will apply in conducting our business. The Disaster Recovery Policy is accessible to all staff via our internal portal Sharepoint and to other interested parties via our customer Dashboards and on request.

Director responsible for Disaster Recovery and Business Continuity, 31st January 2009

