



electrical & fire safety services

BACKUP STRATEGY & DISASTER RECOVERY POLICY

Policy Statement

The purpose of this policy is to set in place strategies to ensure the secure backup and recovery of important data that is stored on the DPL Electrical Services Limited network. The data to backup includes all management data files, administration network user documents, engineering staff documents and Company documents.

The strategies in place will be robust enough to ensure the recovery of data in any circumstance, including fire, catastrophic hardware or software failure, file deletion or virus or hacker attack. Data can be destroyed by system malfunction or accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary.

The ongoing availability of important data is critical to the operation of the business. In order to minimise any potential loss or corruption of this data, people responsible for providing and operating administrative

applications need to ensure that data is adequately backed up by establishing and following an appropriate system backup procedure.

Statement of Authority & Scope

This policy is intended to detail the accepted good practice policies in the backing up and restoring of data on networked computer systems. The Administration Manager provides the framework, design and implementation of backup strategies employed at DPL Electrical Services Limited. The Administration Manager and authorised persons within the Administration Department are then responsible for the operation of these strategies.

The Administration Manager administers this policy with the full support of the Board of Directors.

Full Tape Backups

The following data will be backed up every Friday onto backup tapes

Administration software data files

Administration network user documents

Management Data files

Engineering staff data files

Company data files

Weekly full backup tapes will be retained for two months.

In addition a full backup will be taken on the last day of each month and retained for six months.

These backup tapes to be stored off-site.

Incremental Backups

Incremental backups of all of the above files will be taken, on backup tapes, on Monday through Thursday of each week. (An incremental backup is any backup in which only the files that have been modified since the time of some previous backup are copied) are to be kept, off-site, for a period of two weeks.

Archive Backups

The Company is investigating the possibility of utilising internet data storage as long term solution for archiving the entire DPL Electrical Services Limited ICT facility.

Frequency of Backups

Tape backups are performed every weeknight on each network server. Each backup, which is unattended runs through the night, Incremental backups are performed manually, once a week at the end of the day.

Storage Access and Security

All backup media to be used will be stored in a secure, lockable area that is accessible only to authorised staff. All backups stored off-site will, again, be kept in a secure lockable environment. All backup media that is not re-usable will be destroyed thoroughly in an approved manner. Backup media that is used for other purposes will be erased thoroughly.

Off Site Storage

It is established good practice to keep a full set of backup media stored offsite. In the event of normal backup and restore devices being unavailable due to fire for example, it is imperative that alternative backups are available in a separate location.

Backup Logs

The Administration Manager will monitor backup logs to ensure that network data has been fully backed up. Backups will be regularly tested to ensure that data can be correctly restored.

Backup of data stored on Laptops \ Departmental computers

All data should be stored centrally on the network servers, personal data should be stored in a users home directory. There are instances though where users may want to store their data locally on the computers and \ or laptops hard drive. In this instance it is the responsibility of the user to ensure that their data is backed up. The means of doing this will be dependent on the capabilities of their machine, but could include floppy disk, USB data storage or CD-R.

In the event of a user losing work that is stored locally on a laptop or Desktop PC, the Administration Department using various undelete and disaster recovery software shall attempt recovery of these lost files. The success of this will be very dependent on a mixture of circumstances beyond the control of the Administration Department.

Documentation

It is the responsibility of the Administration Manager to provide documentation on the backup strategies employed at DPL Electrical Services Limited. This will include –

- Date of data backup
- Type of data backup (incremental, full)
- Extent of data backup (files/directories)
- Data media on which the operational data are stored
- Data media on which the backup data are stored
- Data backup hardware and software used (with version number)
- Storage location of backup copies

Disaster Recovery

In the event of a complete network failure, power cut, server breakdown, fire or any other eventuality where the network is unavailable a disaster plan needs to be in place to ensure the continued smooth running of the business. This would include periods when the time taken to restore the network would take more than a day.

The following emergency procedures would need to be in place –

- To ensure that business operations, staff cover, financial transactions and any other critical business management systems can still run the member of staff responsible for these areas should ensure that they have their own disaster recovery plan. This will then enable them to at least continue working in these areas. The person responsible for their particular area should follow the following guidelines in formulating their own disaster recovery plan –
 - Identify essential business management functions. Essential business functions are those functions that must take place in order to support an acceptable level of continuity for the business.
 - Document procedures to implement this disaster recovery plan.
 - Make sure the plan can work effectively in the event of a disaster.

- Make sure staff who work within these critical business management areas are aware of the plan and are able to carry it out effectively.
- Plan for the alternate processing of data to use during a disaster. This would include keeping hard copies of certain data and documents and documentation of any disaster plan.
- Make your Line Manager aware of what strategies would be employed in the event of a disaster.

When the server and network have been restored any new information can then be transferred or entered back into the network system. If a user on the administration network needs to load up an important

document this should be possible due to the fact that extra backups are made independent of the network servers. A user could then work locally (not attached to the network) on their desktop PC or laptop with that document.

When the server and network have been restored any new information can then be transferred or re-entered into the network system.

To provide the maximum protection against the possibility of server failure it is DPL Electrical Services Limited's policy that all network servers that are purchased have built in fault tolerance and redundancy.

Server Backup and Restore

Each server is backed up every weeknight, this backup includes the server operating system, configuration files and in the case of the Primary Domain Controller this would include network data such as usernames, policy and profile data and security information. In the event of complete server operating system failure the server operating system would initially need to be re-installed then the server backup restored. In the event of server hardware failure, the server would first need to be repaired, then the server backup restored.

Data Restoration

Only the Administration Manager and authorised personnel will have access to the means to restore network data. The Administration Manager will determine if a successful restoration is possible.

Any requests for restoration of user data will be made to the Administration Manager.

In the event of complete server failure where a full restoration of Company management software and data files is necessary, a member of the Board will need to give approval.

Alternative Accommodation

DPL Electrical Services Limited will keep an up to date register of all locally available serviced office premises. This register to be kept off-site and to be used to find immediately available office space for the continuation of the business, in the event that the Disaster Recovery Plan has to be implemented.

Replacement of Supplies

It is the responsibility of all operations staff to ensure that, as far as is possible, they have sufficient product and equipment for the discharge of their immediate service to clients. It is the responsibility of the Quality Manager, in the event of a disaster, to locate and replace all items that are either damaged, or lost.
