***Disaster Recovery Plan for Parishes***

A DR plan consists of the policies and procedures that a given entity – in your case, a parish – will follow when disaster strikes. This could be a natural disaster, technological failure or human factors such as sabotage or terrorism. The basic idea is to restore the affected processes as quickly as possible, whether by bringing disrupted services back online or by switching to a contingency system.

**Your DR plan should take into account the following:**

IT services: Which business processes are supported by which systems? What are the risks?

People: Who are the key personnel in a given DR process?

Suppliers: Which external suppliers would you need to contact in the event of an IT outage? Your data recovery provider, for example, Electricity supplier, repair man.

Locations: Where will you work if your normal premises are rendered inaccessible?

Testing: How will you test the DR plan?

Training: What training and documentation will be provided to ensure everyone knows what they have to do?

**Structuring the perfect disaster recovery plan**

Even a small DR plan can be a lengthy and complex document. However, most follow a similar structure, encompassing definitions, duties, step-by-step response procedures and maintenance activities.

Introduction: A summary of the objectives and scope of the plan, including IT services and locations covered.

Roles and responsibilities: A list of the internal and external personnel involved in each DR process covered, complete with their contact details and a description of their duties.

Incident response: When should the DR plan be triggered and by who? How and when should others (PCC, congregation, diocese etc) be notified?

DR procedures: Once the DR plan is triggered, the key personnel can start to action a DR process.

Appendices: A collection of any other lists, forms and documents relevant to the DR plan, such as details on alternate work locations, insurance policies, and the storage and distribution of DR resources. A list of passwords/ bank details, other important information should be included.

**Keeping your disaster recovery plan alive**

Like any policy document, a DR plan is useless if it spends most of its life sitting in a drawer somewhere. There’s no point in creating one if you’re not going to allocate sufficient resources to training personnel on the existence of the plan, as well as what their own roles and responsibilities would be in the event of a disaster.

Keeping it up to date is important, too. As time passes, you’ll need to accommodate new people, new systems and changes in your DR plan. Be sure to notify any affected key personnel when you do this.

Finally, it’s fundamentally important that you test your DR plan and know whether it is viable, or even whether your procedures are fit for purpose at all. It can be tempting to test your DR plan in stages, but don’t neglect to test it in its entirety from time to time, too – it’ll show you if different processes cause friction when they run concurrently, as well as if there’s anything you’ve failed to account for.