Policy Document

Four Business Solutions

Disaster Recovery and Business Continuity Plan

FOUR

BUSINESS

SOLUTIONS

4.

www.four.co.uk

www.four.co.uk

Business Continuance & Disaster Recovery Plan

(As of 1.1.2011)

At Four Business Solutions (Four), our company and brand are built on enabling customers to operate with confidence during normal business operations and in the event of an unexpected incident.

Our goal is to create a control environment that meets or exceeds all expectations, based on regulatory guidelines and industry practices that enable our customers to operate with confidence. The end result of these efforts is a philosophy that ensures that control objectives are developed and implemented on a proactive basis. This philosophy is core to the day-to-day operations of Four Business Solutions and its service providers.

Governance

The governance structure for our business continuance plan is as follows:

- Steering Committee: The steering committee will provide the oversight and authorisation for all projects that are performed as a result of the plan. A review of the plan and progress will be covered with the steering committee at least once per year.
- Executive Sponsor: The executive sponsor will establish the overall direction and approach for the initiative. The executive sponsor will receive frequent updates on progress and assist on issues resolution, if required.

Approach

The scope of this plan is the business operations of Four Business Solutions. As part of the scope, information system services provided by Four control environments will be implemented for all areas of the business to ensure that the control solutions benefit all of the customers and users of Four Business Solutions technologies.

Security

Information security impact is essential to our brand and quality delivery. We have an information security approach that is updated routinely to adapt to the changing environment and technology employed by us.

Four Business Solutions' security and risk approach is managed as a closed loop process. A risk reduction model for data control is established based upon many business drivers for our overall business. A set of security policies and general practices within Four help to guide these protection activities as a whole. The goals are implemented through a variety of activities undertaken by us including process definition, policy setting, hardening standards and procedures, technology investments, and education. The Four Business Solutions operational environment is then audited for compliance to the policies. Remediation action plans are developed to drive our compliance objectives.

Our information security plans cover physical and logical security of our data, application systems, networks, and computing environments. In addition, we have compliance reviews to ensure the effectiveness of the controls. Finally, we leverage our internal and external audit resources to provide an objective review to our information security plan. Any gaps in our information security plan that are identified in these reviews result in management action plans and are diligently addressed.

Business Recovery

Our business continuance program is centred onto minimising disruption to our customers.

Our Business Recovery Plans focus on individual site recovery as well as critical Business Process Recovery. The Disaster Recovery plans are tested on a semi-annual basis with action plans established to address issues from the test. The tests validate the procedures and note any changes or modifications that are required. These items, along with general maintenance (e.g., organisational changes, vendor contacts, etc.), are included in the regular plan maintenance process. Planning for the next test commences at the end of the maintenance process. This lifecycle approach ensures the business recovery plans are continually updated.

Within our primary Information Centre, redundant systems are in place for critical infrastructure to handle simple short term outages:

- Electrical and mechanical systems
- Redundant air conditioning for continuous cooling of computer equipment

Our business continuance program is based on sound disaster avoidance practices for our critical systems.

Data Backup Process

Four Business Solutions has invested in the IT infrastructure to provide redundancy and fault tolerance. Servers are configured as multiple systems operating in a VMware environment. Web and midrange systems are clustered with load balancing and fail-over capability at a warm site.

Network Area Storage devices with Business Continuity Volumes. These volumes are replicated to our recovery environment on a weekly basis and stored on a remote storage device to meet our recovery time objective. All recoverable BCV's are also sent to our offsite storage location.

For security Four Business Solutions utilises a dual layer DMZ and intrusion detection systems at both the primary and backup Web Hosting sites. We have comprehensive incident planning in place that covers a multitude of potential situations from routine to disaster. These plans include evacuation procedures, communications plans, alternative recovery contingencies and failover plans for key business capabilities.

Additional Detail about Four Business Solutions' back-up capabilities:

- Full data backups are made weekly. - Offsite
- Weekly replication on specific systems to our remote disaster recovery site.
- Monthly replication on all systems is maintained at our offsite data protection provider.

Recovery of Declared Disaster

Our business recovery plan has provisions to enable us to restore our critical databases, data centre operations and telecommunications capabilities within 48 hours in the event an unexpected incident renders our computer facility unusable.

The recovery plan includes detailed steps for the declaration of a disaster through the resumption of services.

- Areas covered in the recovery plan: (48 Hour RTO)
  - Escalation and Notification Procedures
  - Hot-Site Facility Notification Process
  - Offsite Storage Facility Notification – delivery within 2 hours
- Perform Detailed Damage Assessment
- Establish Command Center
- Activate Recovery teams
  - Telecommunications recovery
  - Technical recovery

    - Storage Management recovery
    - Applications recovery
    - Database recovery
    - Production Operations recovery
- Perform Application/System recovery at alternate recovery location.
- Establish Customer facing application access.

A detailed business recovery document covers these and other steps to re-establish the functionality of the primary office in the event of disaster. This document is considered confidential and customer copies are not permitted. These plans include evacuation procedures, communications plans, alternative recovery contingencies and failover plans for key business capabilities.