Information Technology Security Policy – Electronic Data Backup

To be read in conjunction with IT Security Policy

Electronic Data Backup Principles

The Key Conference Solutions Information Technology Security Policy requires scheduled backups of data, including email, client correspondence, client data, venue data,

The Electronic Data Backup Policy and Procedure is committed to and guided by the principles of ensuring that:

- Data necessary to support the company's operations will be kept and retained on a network drive.
- Data necessary to support the company's operations will not be stored on local PCs.
- The company and staff will take back-ups of data on a regular basis and ensure that data can be recovered to the latest version in the event of deletion, corruption or other loss of data.
- Back up cycles, retention periods and target recovery objectives will be determined in conjunction with the business owner of each application.

And ensuring staff are aware that:

- Data stored in locations other than the network cannot be guaranteed against loss. Faults and IT support requirements may necessitate re-imaging or erasing of equipment. As a result all data on that device may be lost at any point.

Policy

The Information Technology Manager is responsible for ensuring that Backup procedures are observed as defined.

Data storage

- Company data will be stored and retained on network drives unless other suitable backup arrangements have been determined and approved by Information Technology Manager.
- Data will not be removed from network drives unless it has been determined that this data will no longer be required.
- Company data will not be stored on local PC drives unless it is fully backed up to a suitable network location.

Data Backups

- Information Technology Manager will manage and control backups of the company's server and core database and technology infrastructure and ensure that business data is secure, protected and can be restored or retrieved with minimal disruption to operations.
- Information Technology Manager will automatically take backups of all staff data stored on:
    - Key Conference Solutions file servers
    - Key Conference Solutions application servers
    - Key Conference Solutions Linux/Unix/Windows/OSX servers
    - Key Conference Solutions email servers
    - Key Conference Solutions database servers
- Unless specifically requested, data stored on non-production systems will not be backed up.
- Important data not included in automated backups must be manually backed up and restorable in the event of a breach of security, deletion or corruption of data or hardware failure.

Exclusions

- Data stored on desktops, notebooks, hand held computers and USB storage devices will not be backed up by the company.

- Staff acknowledge that any data not stored on company servers may be lost at any point with no ability to recover unless they have taken their own back-ups of data stored on these devices.

Externally hosted systems

Systems hosted off site will be backed up by the vendor at the time the hosting service is arranged. Basic criteria for any third party hosting server will be inclusive of vitualisation enabling restoration of data and data functions with minimal interruption. Company and client data stored on an external server will be backed up daily to the company internal system.

Recovery testing

Backups will be periodically tested to ensure recoverability of data

Data security

All systems used to store company or client data will be protected by appropriate security services including firewall, user access and authorisation restriction and virus scanning software.

Procedure

Data storage

Storage of company, user and client data

- Ensure company, user and client data is stored in an appropriate network location and secure access granted to employees requiring access

- Take reasonable steps to ensure data to be deleted / removed from network locations will not be required in the future.

Data backup

Backups

- Document and update as required, default Backup and recovery standards for company systems.

- Document Disaster Recovery plans for company systems.

- Take Backups of all employee data stored on network drives and servers consistent with identified Backup standards or requirements.

- Store all Backup media in a secure area with access by authorised personnel only

- Publish and maintain a list of network locations included in automated Backup system

- Take regular Backups of any Important Data stored on desktops, notebooks, hand held computers, USB storage devices, etc. This may occur through copying up to a network location included in the automated Backup system.

Externally hosted systems

- Provide advice on the adequacy of Backup and recovery processes proposed for externally hosted solutions.

- Ensure any systems hosted off-site have, if required, an appropriate and periodically tested Backup and Recovery process

Recovery testing

- Periodically test recoverability of data stored in manual Backups held in locations other than one included in the automated Backup system.

- Periodically test Backups and Disaster Recovery Plans for automated Backups

Data security

- Protect company owned systems.

- Protect personal systems.