End-User Backup Policy

Introduction

Data is one of USEK's most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on company desktop computers, PCs, and PDAs – as well as home office/mobile devices and appliances – will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

Scope

This policy refers to the backing up of data that resides on individual PCs, notebooks, PDAs, laptop computers, and other such devices (to be referred to as "workstations"). Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is imperative that end-users save their data to the appropriate media and/or network space outlined in this policy, in order that their data is backed up regularly in accordance with company regulations and business continuity plans.

This policy does not cover end-user information that is saved on a network or shared drive, as these are backed up when the servers are backed up. For information on how often the IT department backs up servers, please refer to USEK's Server Backup Policy.

Backup Schedule

Backups are conducted automatically Microsoft Data Protection Manager 2007.Backups must be conducted every day at 1:30 PM.

Data Storage

It is USEK's policy that ALL corporate data will be backed up according to schedule. This includes any company documentation (i.e. reports, RFPs, contracts, etc.), e-mails, applications/projects under development, Web site collateral, graphic designs, and so on, that reside on end-user workstations.

- **Office Users:** Corporate data, especially work-in-progress, should be saved to a specific drive after consent of IT, located on the company network by in-house employees. This ensures that data will be backed up when the servers are backed up. Users in branch offices will do the same, via the company's Wide Area Network (WAN). However, if data is saved on a workstation's local drive, then that must be backed up every week onto storage media such as CD Read/Write disks or some type of removable storage device, such as a mini hard drive, data cartridge, or solid state memory card.

- **Remote/Mobile Users:** Remote and mobile users will also back up data to a specific drive after consent of IT, provided they have access to the drive via a Virtual Private Network (VPN) connection. Where a VPN is not in use, the remote/mobile user will download his/her device's data to their in-house computer every 4 days, and then follow the *same procedure* as "Office Users" shown above. If this is not feasible, due to distance from his/her office, then the remote/mobile user will employ CD Read/Write disks. Should Read/Write disks not be available, then select files should be copied to some type of removable storage device, such as a mini hard drive, data cartridge, or solid state memory card.

Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential that the IT department regularly tests its ability to restore data from the storage media or network drive. As such, all storage media must be tested at least once every month, to ensure that the data they contain can be completely restored to end-user workstations.

Data will be restored from a backup if:

- There is an intrusion or attack.
- Files have been corrupted, deleted, or modified.
- Information must be accessed that is located on an archived backup.

In the event that an end-user requires or desires a data restore, the following policy will be adhered to:

1. The individual responsible for overseeing backup and restore procedures is Elie Eid. If a user has a restore request, they can contact Elie Eid by calling 1435, or sending an e-mail to elieeid@usek.edu.lb

2. Mobile and/or remote users will likely be carrying their backups with them. In the event that a restore is needed, the user will contact USEK's IT Service desk at servicedesk@usek.edu.lb. The IT Service desk will walk the user through the restore procedure for their mobile device.

3. In the event of unplanned downtime, attack, or disaster, consult USEK's Disaster Recovery Plan for full restoration procedures.

4. In the event of a local data loss due to human error, the end-user affected must contact the IT Department and request a data restore. The end-user must provide the following information:

    - Name.

- Contact information.
- Name of file(s) and/or folder(s) affected.
- Last known location of files(s) and/or folder(s) affected.
- Extent and nature of data loss.
- Events leading to data loss, including last modified date and time (if known).
- Urgency of restore.

5. Depending on the extent of data loss, backup tapes and storage media may both need to be used. The timing in the cycle will dictate whether or not these tapes and/or other media are onsite or offsite. Tapes and other media must be retrieved by the server administrator or pre-determined replacement. If tapes and/or other media are offsite and the restore is not urgent, then the end-user affected may be required to wait up to three business days for a time- and cost-effective opportunity for the tape(s) and/or other media to be retrieved.

6. If the data loss was due to user error or a lack of adherence to procedure, then the end-user responsible may be required to participate in a tutorial on effective data backup practices.

Declaration of Understanding

I, [employee name], have read, understand, and agree to adhere to USEK's End-User Backup Policy.

Name (Printed): _____

Name (Signed): _____

Today's Date: _____