PASSWORD POLICY

1. Purpose.

1.1. The main purpose of this policy is to have a standard password system (in accordance to Industry best-practices) in place to ensure the security of confidential official data. Effective implementation of the Password Policy will minimize risk from password cracking or guessing and ensure the Confidentiality, Integrity and Availability of data.

2.1. This policy applies to all employees (who have access to official computer systems and confidential data)

3. Policy.

3.1. All users should be responsible for managing the passwords of their systems.

3.2. Users should their change their default password allotted by the administrator, on their first log-in.

3.3. The password should be alphanumeric. The password should be a combination of upper and lower case, should have punctuation characters as well as letters, for example the following characters can be used along with letters: 0-9,!@#$ %^&*()_+|~-=\`{}[]:";'<>?,./)

3.4. The complexity of the password should vary with the level of Information that it is used to protect.

3.5. The length of the password should be minimum eight (8) characters. It should not be any word from the dictionary or formed in any known pattern like a1b2 etc.

3.6. The server password should be changed every 15 days and other passwords should be changed in 30 days. The system should remember last 5 passwords.

3.7. The password should not be disclosed to any other person either over the phone, mail or any other medium.

3.8. The “remember password” feature present in applications and browsers should not be used.

3.9. As good practice passwords for official mail account and non-official mail personal accounts should be different.

4. Responsibilities.

4.1. All employees should be aware of the Password Policy and it will be the responsibility of the Administrator to ensure employee awareness for the same.

5. Enforcement

5.1. Any employee/user found to have violated this policy should be subject to disciplinary action as per the rules of the organization.

6. Amendment/Termination of this policy.

6.1. Company reserves the right to modify, amend or terminate this policy at any time.

Back up storage and retrieval Policy

I Purpose and Scope of the Policy

The purpose of this policy is as follows:

•To provide secure storage for data assets critical to the work flow of official business

•To prevent loss of data in the case of accidental deletion / corruption of data, system failure, or disaster

•To permit timely restoration of archived data in the event of a disaster or system failure

This policy applies to all computers, both mobile and desktop, owned by the company

•Specific locations will be automatically backed up(e.g., My Documents, Desktop, Bookmarks)

•Any location outside of the automated backup locations will be added on a per request basis

Backups are NOT meant for the following purposes:

• Maintaining a versioned history of data

•Personal data such as photos, videos, music, non-brown e-mail accounts, etc.

•Programs (i.e., applications) of any type (personal or officially supported)

•Exceptionally large images (scanned or digitized material) and large video files. If you need this type of storage space, please contact Administrator to discuss alternative backup options available.

II. Backup and Recovery Policy

Data

The following resources are made available to backup critical files pertaining to official

- \\filese._users - scroll down to your user folder (e.g., rajiv)

Secure storage forstaff documents, presentations, spreadsheets, etc. pertaining to official business.

\\filese.ad.brown.edu\library_shared- scroll to dept. folder (e.g., _Systems_Office)Secure storage for departmental and shared usage.

External USB hard driveUtilizing Microsoft Backup or Apple's Time Machine to backup u ser folders that are in excess of the TWO Gigabytes. A member from Administering will perform the initial configuration and schedule a backup policy. All external drives must b e locked in a secure location at the end of the work day.

USB Thumb diveNot supported as an official means of backup. These devices can easil y be misplaced or lost resulting in the potential breach of official data. If utilized, the data must be encrypted if taken off the premises.

Archived E-mail

The company has recently moved to Googleapps for e-mail
and has provided a dynamically growing 7+ Gigabytes of e-mail
storage (including attachments). If your archived e-mail is larger than the allotted storag e space, it will be treated on a case-by-
case basis. Company is also actively searching for a service thatsupports online e-mail archival for more than 7 Gigabytes.

Archived e-mail stored on your computer's hard drive is not backed up if it does not fit on e of the templates in the data backup policy above. Please contact someone from Admin istration to assist with a backup option.

Backup Schedule and Retention

The Network backup system is utilized to retain data for 6 weeks or 42 days. A combination of incremental and full backups is executed on the dataset. A full backup is performed every Friday with incremental backups thereafter.

This creates a scenario where Company can restore a folder like \\filese._shared_syste ms_office to a single point in time in the past up to a maximum of 42 days.

Software

Windows Operating System:

Microsoft Backup is utilized to backup to, restore from, and verify data on the PC platform

TrueCrypt – open source on-the-fly data encryption for drives (provide more

detail…)

AxCrypt – open source file level encryption

Macintosh Operating System:

Time Machine is utilized to backup to, restore from, and verify data on the Macintosh plat form

TrueCrypt –
open source on-the-fly data encryption for drives (provide more detail…)Backup and Recovery Policy 2011

Systems Office

File Vaultis utilized to encrypt at the file level using AES-128 bit encryption

Verification

If configured properly, both Time Machine and Microsoft Backup will perform a full verification against a backup set after every job to protect against corrupted data. No oth er form of verification is scheduled or performed.

Data Restoration

Emergency recovery:Systems staff will make every attempt torecover the data within a b usiness day. However, in the event of a catastrophic event,
such as fire damage,services and data may be unavailable for an extended period of time.
Non-Emergency recovery: These restorations will be performed on a time available basi s, and will occur within the next five business days.

Required Information:

Users that need files restored must submit a help desk ticket request or contact System dept. The detail of the request should include information about
the file creation date, the name of the file, the last time it was changed, and
the date and time it was deleted or destroyed.
Any lost data not backed up is beyond the scope of this document
You are responsible for saving files to the specified backup Directories.

****