Syrian American Medical Society Foundation

Staff Data Storage Policy

Contents

Version Control:

Date	Version	Author(s)	Comments

1. Introduction

1.1 SAMS has a responsibility to maintain the confidentiality, integrity and availability of its stored electronic data (documents, emails etc.). To this end, all organization electronic data is held on the: Turkey - Storage Area Network (SAN), Jordan – Network Attached Storage (NAS), which is highly resilient and is backed up every day to Google drive account. However, SAMS is aware that improper use of corporate technology, e.g. the storage of personal, offensive or defamatory emails, documents, photographs and multimedia files could have the following effects:

a) It could expose both SAMS and the user to potential legal liability
b) It may infringe copyright laws

1.2 Consequently, SAMS is aware of the need to regulate use of the organization infrastructure for the storage of personal data.

2. Internal Network Storage

The following general principles apply:

2.1 SAMS data storage infrastructure includes any digital media used within the Authority, including, but not limited to, disks, tape or other media installed as part of the SAN/NAS, network servers, desktop PC's and laptops, portable hard disks, USB memory sticks and flash memory cards.

2.2 The primary use of SAMS storage infrastructure is to store, retain and secure organization data.

2.3 Personal folders should be used only for the storage of work, related documents which are specific to the users' post or job function; shared or group data should be held in the workgroup data area (see 2.4 below).

2.4 Workgroup folders are designed to be used by employees who share document templates, reference documents, spreadsheets, databases, photographs etc. Access to these folders can be restricted to specific groups of employees thus maintaining security and privacy for confidential data. Sharing also helps to eliminate duplication of files across the infrastructure and can be set up by ICT staff on request. In Jordan, shared folders is accessed by Domain users.

2.5 The storage infrastructure should not be used to store personal data (personal data is data created and/or held in respect of an individual's personal and/or private capacity) and in particular any form of data which is pornographic, defamatory or racially or otherwise abusive.

2.6 Specifically, the following types of personal data must never be stored on SAMS storage:

- Personal documents or email
- Personal digital photos
- Video clips, MP3 or other audio files
- Music libraries, e.g. iPod
- Animated files. E.g. Flash, Shockwave and similar files
- Copyright material without the permission of the copyright holder

2.7 Exceptions to the above can be made for work related purposes such as research for projects, data for a work related qualification (at the discretion of the officer's line manager, such permission not to be unreasonably withheld).

2.8 SAMS respects the copyright of those involved in creating and disseminating copyright material, such as music, films, software, and other literary and artistic works created by others. SAMS employees shall not make, store, transmit or make available illicit copies of such copyright material on SAMS data infrastructure, equipment or storage media.

2.9 SAMS staff shall not upload, store or make available unauthorized copies of copyright material via SAMS local area network or the internet using SAMS systems, equipment or storage media.

2.10 Permission for the use of such material must be obtained prior to the use and the line manager must keep a written record of the authorization.

2.11 SAMS reserves the right to monitor staff use of the data storage infrastructure to ensure lawful use in accordance with this policy.

2.12 Data storage monitoring will be carried out only so far as to ensure proper use of the facility, and in particular to stop inappropriate or unlawful use or to prevent its use in criminal activities.

2.13 SAMS reserve the right to delete any unauthorized data from the infrastructure without approval of the originator.

2.14 Staff transferring data from our network via portable media must conform to the SAMS's ICT Security policy.

3. Cloud based Storage

3.1 Cloud Storage definition and risk

3.1.1 The phrase "cloud storage" can be defined as any third party solution which stores information to an online storage facility such as Google Drive, Dropbox and OneDrive.

3.1.2 Files stored on these services can usually be accessed via any web browser and have the facility to share files with other people. Whilst being attractive, offering excellent features that are easy to use, they bring with them a series of risks to SAMS which must be considered.

3.1.3 Using the "cloud" to store data for work purposes is a potential security risk. Staff must follow the guidance in this policy to limit the risk imposed on Council data.

3.1.4 The main risks when files are stored in public cloud storage are that:

- SAMS can no longer guarantee the quality of access controls protecting the data
- In many cases, public cloud storage required that files be associated with an individual's personal account. Should that individual become ill, be absent for other reasons or leave, SAMS could lose access to the data.

- Cloud services generally limit their liability for negligence, resulting in little or no recourse should the provider misuse, lose or damage information stored in the cloud
- Few cloud providers guarantee that they will not access the information stored within their service, leading to concerns over privacy and intellectual property rights
- Some if not all providers guarantee that the user's ownership of the data stored in the cloud will be retained. This is primarily to enable the provider to move data around to their different server locations without your prior approval but opens further questions about intellectual property rights
- Using cloud storage software to synchronize files between work and personal devices could result in personal/sensitive information being held inappropriately on personal equipment
- If they have financial difficulties, a cloud storage provider may end the service with little or no notice, leaving staff with no access to files.

3.1.5 All data that is generated as part of staff duties belongs to SAMS and must be managed in line with this policy. Using cloud services may require you to transfer ownership of SAMS data, which you may not be eligible to do.

4. Further Advice

4.1 Employees can get further advice on the issues outlined in this policy by contacting ICT officer via: maleid@sams-usa.net (Turkey) Bassam.khlifat@sams-usa.net (Jordan)

4.2 Failure to comply with the policy, and deliberate or persistent abuse of the system, may result in disciplinary action. This protocol forms part of your conditions of service and any breaches may be treated as a disciplinary matter.