



Co-funded by
the European Union



I.MAM
VIRTUAL



Co-funded by
the European Union



LESSON 7

DATA BACKUP

I.MAM VIRTUAL – 101083431 Programme(s): Erasmus+ (ERASMUS+) Topic(s): ERASMUS-EDU-2021-VIRT-EXCH-NDICI Type of action: ERASMUS Project Grants ERASMUS-EDU-2021-VIRT-EXCH- Virtual Exchanges



What is Data Backup?

Data backup is the process of creating copies of data to protect against data loss. These copies can be used to restore the original data in case of hardware failure, accidental deletion, or other data loss events.

Importance of Data Backup

Backing up data is crucial to ensure that important information is not permanently lost. Regular backups can save time and money and protect against data breaches and cyber-attacks.



Types of Data

Backup There are several types of data backup, including:

- **Full Backup:** A complete copy of all data.
- **Incremental Backup:** Only copies data that has changed since the last backup.
- **Differential Backup:** Copies data changed since the last full backup



Backup Methods

- **Full Backup:**

A full backup is the most comprehensive type, creating a complete copy of all data. It requires the most storage space and time to complete.

- **Incremental Backup:**

An incremental backup saves only the data that has changed since the last backup (whether it was full or incremental). It is faster and requires less storage space than a full backup.

- **Differential Backup:**

A differential backup saves data changed since the last full backup. It requires more storage space than an incremental backup but less than a full backup.



Backup Media

- **External Hard Drives**

External hard drives are a popular choice for backups due to their large storage capacity and ease of use. They connect via USB or other ports.

- **Cloud Storage**

Cloud storage services like Google Drive, Dropbox, and OneDrive offer online backup solutions, providing remote access and disaster recovery options.

- **Network Attached Storage (NAS)**

NAS devices are dedicated file storage units connected to a network, allowing multiple users and devices to store and retrieve data.

- **USB Flash Drives**

USB flash drives are portable and easy to use, suitable for small to medium-sized data backups.

- **Optical Media (CDs/DVDs)**

Optical media, though less common today, can be used for long-term storage of important data.



Backup Software

- **Built-in Operating System Tools**

Most operating systems come with built-in backup tools, such as Windows Backup and Time Machine for macOS.

- **Third-Party Software**

There are numerous third-party backup solutions available, offering advanced features and customization options.

- **Cloud-Based Solutions**

Cloud-based backup services provide offsite storage and automated backups, ensuring data is protected from local disasters.



Creating a Backup Plan

- **Assessing Your Data**

Identify the critical data that needs to be backed up, considering its importance and frequency of change.

- **Frequency of Backups**

Determine how often backups should be performed based on how frequently the data changes and its importance.

- **Automating Backups**

Automate the backup process to ensure regular and consistent backups without manual intervention.

- **Verifying Backups**

Regularly verify the integrity of backups to ensure that data can be successfully restored



Data Recovery

- **Restoring from Backup**

Learn the steps to restore data from a backup, ensuring you can quickly recover lost information.

- **Disaster Recovery Plan**

Develop a disaster recovery plan to address data loss scenarios and ensure business continuity.

- **Testing Recovery Procedures**

Regularly test recovery procedures to confirm that backups can be successfully restored. Data Recovery Restoring from Backup Learn the steps to restore data from a backup, ensuring you can quickly recover lost information. Disaster Recovery Plan Develop a disaster recovery plan to address data loss scenarios and ensure business continuity. Testing Recovery Procedures Regularly test recovery procedures to confirm that backups can be successfully restored.



Best Practices

- **Regular Backups**

Perform backups regularly to minimize data loss and ensure recent data is protected.

- **Offsite Storage**

Store backups offsite to protect against local disasters such as fire or theft.

- **Encryption**

Encrypt backups to protect sensitive data from unauthorized access.

- **Keeping Backup Software Updated**

Regularly update backup software to ensure compatibility and security.



Co-funded by
the European Union

thank you!



“Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.”