Masterclass Certificate in Digital Archives Organization

Principles of Digital Preservation

Digital preservation is a critical aspect of modern archival practice, ensuring the long-term accessibility and usability of digital materials. In this Masterclass Certificate in Digital Archives Organization, we will explore key terms and vocabulary essential to understanding the principles of digital preservation.

1. Digital Preservation:
Digital preservation refers to the series of managed activities necessary to ensure continued access to digital materials for as long as they are required. It involves the use of strategies, policies, and actions to ensure the integrity, authenticity, and usability of digital assets over time.

2. Born-Digital:
Born-digital refers to materials that are created in a digital format, rather than being digitized from a physical format. These materials include emails, websites, social media content, and digital photographs.

3. Digital Object:
A digital object is a unit of information created or stored in a digital form. It can be a file, a collection of files, or a complex data structure. Digital objects are the building blocks of digital archives and repositories.

4. Metadata:
Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. In digital preservation, metadata is crucial for understanding the context and characteristics of digital objects.

5. Migration:
Migration is the process of moving digital objects from one hardware or software environment to another while maintaining the authenticity, integrity, and functionality of the objects. It is a key strategy for long-term digital preservation.

6. Emulation:
Emulation involves recreating the original hardware or software environment in which digital objects were originally created or accessed. This approach allows for the continued access and use of digital objects that rely on specific software or hardware.

7. Fixity:
Fixity refers to the property of a digital object that ensures it has not been altered or corrupted. Fixity checks are essential for verifying the integrity of digital objects over time and detecting any unauthorized changes.

8. Accession:
Accessioning is the process of formally accepting digital materials into an archive or repository, including documenting their provenance, creating metadata, and assigning unique identifiers. It is the first step in the

digital preservation workflow.

9. Bitstream Preservation:
Bitstream preservation focuses on preserving the exact sequence of bits that make up a digital object, ensuring the integrity of the file itself. This approach is essential for preventing data loss and corruption.

10. Trusted Digital Repository:
A trusted digital repository is an organization that meets specific criteria for the long-term preservation of digital materials, including adherence to standards, best practices, and audit requirements. Trusted repositories provide a secure environment for digital objects.

11. File Format:
A file format is a standard way of organizing and storing data in a digital file. Different file formats have specific characteristics and features, which can impact the long-term preservation and accessibility of digital objects.

12. Obsolescence:
Obsolescence refers to the process by which hardware, software, or file formats become outdated and no longer supported. Obsolescence poses a significant challenge to digital preservation, as it can lead to the loss of access to digital materials.

13. Digital Curation:
Digital curation involves the selection, preservation, maintenance, and archiving of digital assets to ensure their long-term value and accessibility. It encompasses a range of activities, including appraisal, arrangement, description, and storage.

14. Preservation Metadata:
Preservation metadata is a specialized type of metadata that captures information about the preservation processes applied to a digital object. It documents actions taken to ensure the long-term integrity and usability of digital materials.

15. Dark Archive:
A dark archive is a secure storage facility for digital materials that are not actively accessed but are preserved for long-term retention. Dark archives are used for disaster recovery, data protection, and preservation purposes.

16. Digital Rights Management (DRM):
Digital Rights Management is a set of technologies and strategies used to control access to digital content and protect intellectual property rights. DRM can impact the long-term accessibility and preservation of digital materials.

17. Web Archiving:
Web archiving is the process of collecting and preserving web content for long-term access and research purposes. It involves capturing websites, social media content, and other online materials to document the evolving digital landscape.

18. Preservation Policy:
A preservation policy is a formal document that outlines an organization's strategies, procedures, and responsibilities for the long-term preservation of digital materials. It guides decision-making and ensures consistency in preservation practices.

19. Digital Forensics:
Digital forensics is the practice of collecting, analyzing, and preserving digital evidence for investigative purposes. It involves using specialized tools and techniques to recover and examine data from digital devices.

20. Risk Management:
Risk management is the process of identifying, assessing, and mitigating potential threats to the long-term preservation of digital materials. It involves developing strategies to protect against data loss, corruption, and other risks.

In this Masterclass Certificate in Digital Archives Organization, we will delve into these key terms and concepts to build a solid foundation in digital preservation principles. Understanding these terms is essential for effectively managing and preserving digital materials in today's digital age.