österreichischemediathek
audiovisuelles archiv · technisches museum wien

Digitale Langzeitarchivierung an der österreichischen Mediathek

KP-Stakeholderforum 17.10.2024

Digitale Langzeitarchivierung

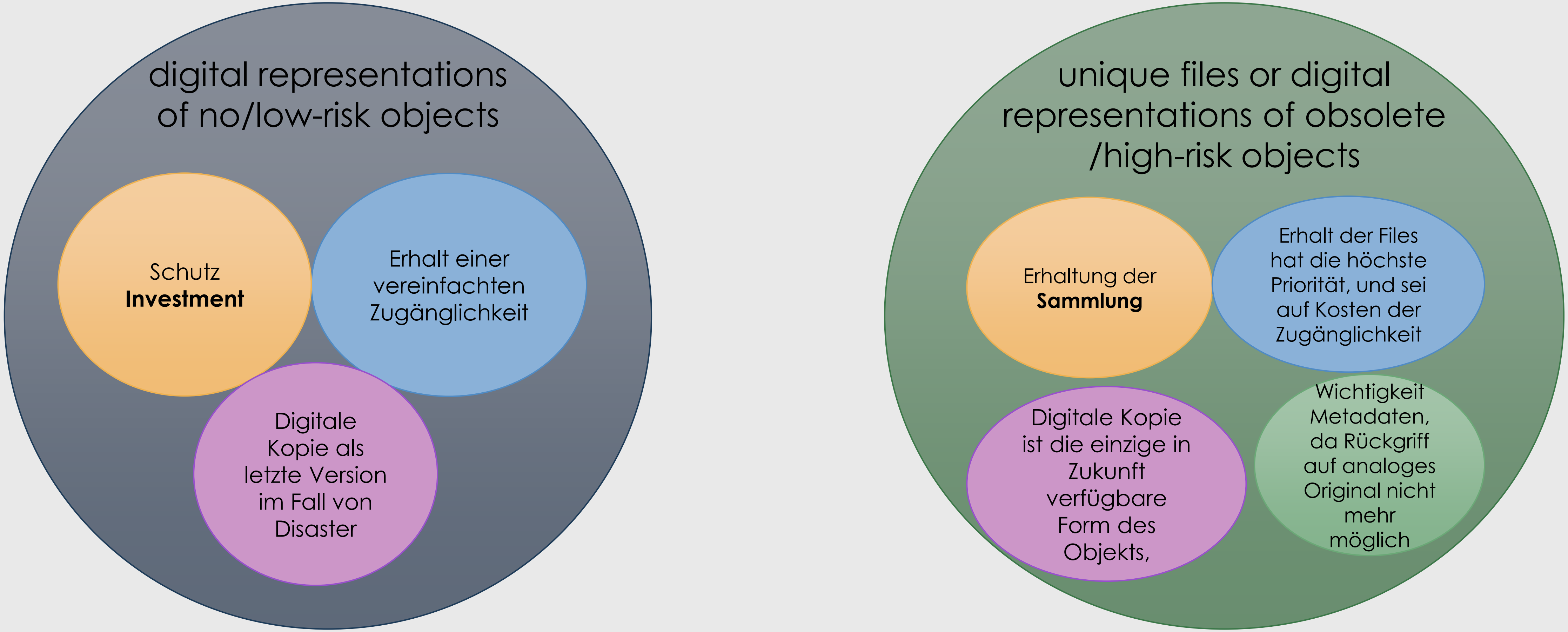
Langzeitarchivierung geht über die reine Speicherung von Daten hinaus (≠ Backup)

LZA hat folgende Ziele:

- Archivierte Inhalte müssen verfügbar und verstehbar gehalten werden
- Inhalte und Eigenschaften der Objekte müssen systemunabhängig verfügbar bleiben
- Die Erhaltung der Nutzbarkeit von Daten über die Lebenszyklen unterschiedlicher Speichersysteme und Formate hinweg

Digitale Archivierung: *Archivierung im Archiv ist immer Langzeit…*

Digitale LZA - Wozu?



digital representations of no/low-risk objects

Schutz **Investment**

Erhalt einer vereinfachten Zugänglichkeit

Digitale Kopie als letzte Version im Fall von Disaster

unique files or digital representations of obsolete /high-risk objects

Erhaltung der **Sammlung**

Erhalt der Files hat die höchste Priorität, und sei auf Kosten der Zugänglichkeit

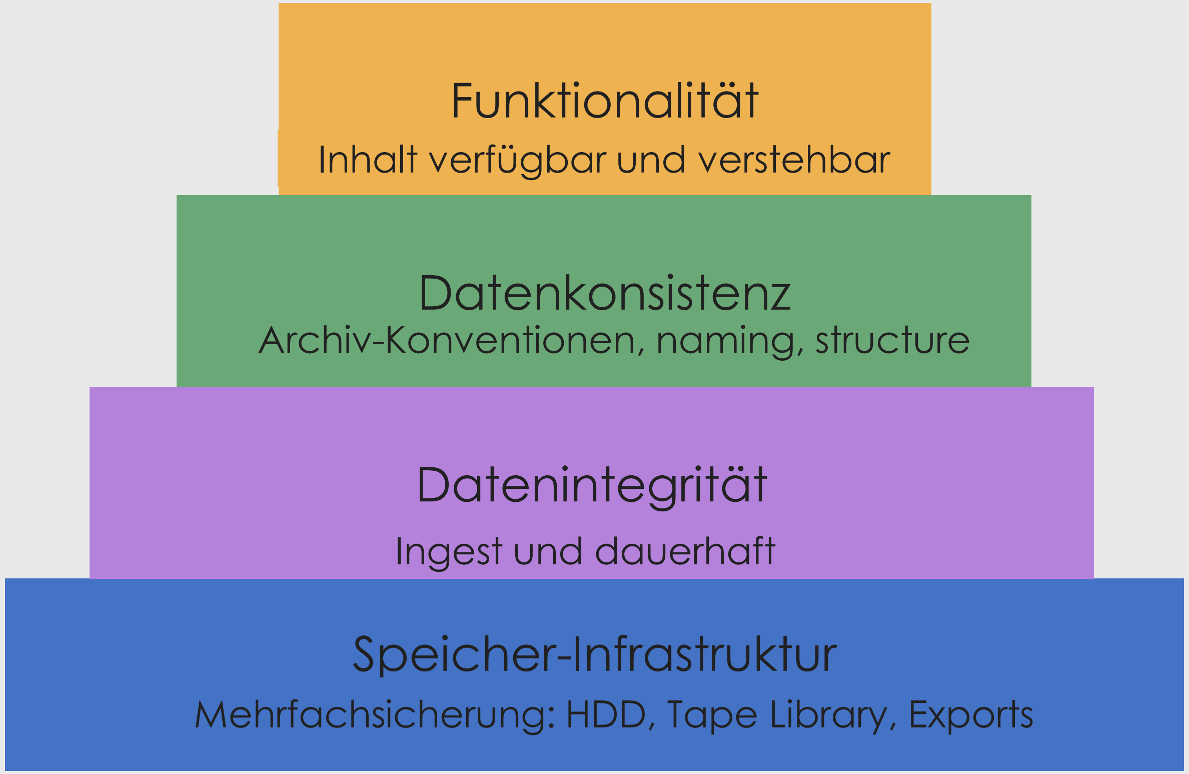
Digitale Kopie ist die einzige in Zukunft verfügbare Form des Objekts,

Wichtigkeit Metadaten, da Rückgriff auf analoges Original nicht mehr möglich

Digitale LZA im Medienarchiv (Audio/Video)

- Prämisse: in Zukunft ist die Abspielbarkeit der Originale unwahrscheinlich
- Audio/Videoarchiv operiert vor dem Hintergrund von Verlust
- Obsoleszenz der analogen Träger und Verlust geeigneter Abspielumgebung
- Ohne Digitalisierung und LZA droht der Totalverlust der gefährdeten Bestände
- Große Datenmengen im Medienarchiv im Vergleich zu Bild, Textdaten
- (Magnetbandbasiertes) AV-Archiv ist in einem Transformationsprozess vom Analogarchiv zum Digitalarchiv
- Kopienerstellung braucht Zeit
- Integritätsprüfungen brauchen Zeit und Rechenleistung
- Hoher Anspruch an Infrastruktur Rechenleistung, Datenleitungen

LZA in der Praxis



Funktionalität

Inhalt verfügbar und verstehbar

Datenkonsistenz

Archiv-Konventionen, naming, structure

Datenintegrität

Ingest und dauerhaft

Speicher-Infrastruktur

Mehrfachsicherung: HDD, Tape Library, Exports

LZA in der Praxis

Sind die digitalen Objekte meiner Sammlung …

- valide?
- komplett?
- intakt?
- funktional?

MEDIAS

Archivmonitoring an der Österreichischen Mediathek

Idee, Konzept and project lead:
Velibor Kojic
IT Technisches Museum Wien mit Österreichischer Mediathek
velibor.kojic@mediathek.at

searchIT https://www.searchit-enterprise-search.com/

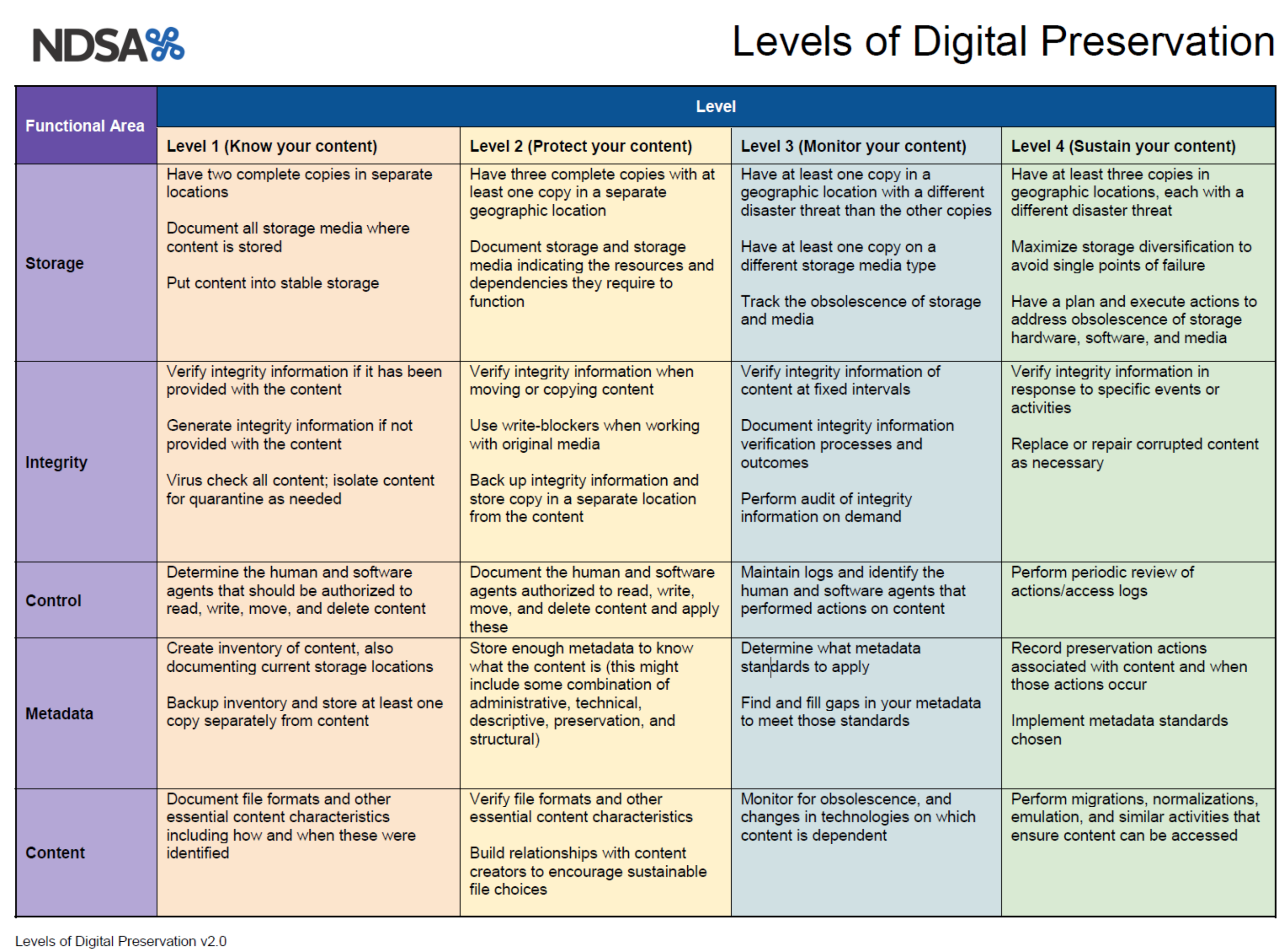
OEM's MEDIAS basiert auf der Software „searchIT" der Firma Iphos

Elasticsearch Kibana Apache ManifoldCF™

search engine reporting process management

Levels of Digital Preservation

https://ndsa.org/publications/levels-of-digital-preservation/



Levels of Digital Preservation

Functional Area	Level			
	Level 1 (Know your content)	Level 2 (Protect your content)	Level 3 (Monitor your content)	Level 4 (Sustain your content)
Storage	Have two complete copies in separate locations Document all storage media where content is stored Put content into stable storage	Have three complete copies with at least one copy in a separate geographic location Document storage and storage media indicating the resources and dependencies they require to function	Have at least one copy in a geographic location with a different disaster threat than the other copies Have at least one copy on a different storage media type Track the obsolescence of storage and media	Have at least three copies in geographic locations, each with a different disaster threat Maximize storage diversification to avoid single points of failure Have a plan and execute actions to address obsolescence of storage hardware, software, and media
Integrity	Verify integrity information if it has been provided with the content Generate integrity information if not provided with the content Virus check all content; isolate content for quarantine as needed	Verify integrity information when moving or copying content Use write-blockers when working with original media Back up integrity information and store copy in a separate location from the content	Verify integrity information of content at fixed intervals Document integrity information verification processes and outcomes Perform audit of integrity information on demand	Verify integrity information in response to specific events or activities Replace or repair corrupted content as necessary
Control	Determine the human and software agents that should be authorized to read, write, move, and delete content	Document the human and software agents authorized to read, write, move, and delete content and apply these	Maintain logs and identify the human and software agents that performed actions on content	Perform periodic review of actions/access logs
Metadata	Create inventory of content, also documenting current storage locations Backup inventory and store at least one copy separately from content	Store enough metadata to know what the content is (this might include some combination of administrative, technical, descriptive, preservation, and structural)	Determine what metadata standards to apply Find and fill gaps in your metadata to meet those standards	Record preservation actions associated with content and when those actions occur Implement metadata standards chosen
Content	Document file formats and other essential content characteristics including how and when these were identified	Verify file formats and other essential content characteristics Build relationships with content creators to encourage sustainable file choices	Monitor for obsolescence, and changes in technologies on which content is dependent	Perform migrations, normalizations, emulation, and similar activities that ensure content can be accessed

Levels of Digital Preservation v2.0