Chain of Custody

Knowing who has handled a tape and when it was handled has always been considered good practice, but in recent years corporate governance, privacy, information handling and critical infrastructure laws have been introduced[1] in many jurisdictions. It is expected that further laws will be passed in the future.

In addition to this, over the past decade Common Law precedents have been established that specifically acknowledge the importance of retaining a constant chain of custody within tape management[2].

In developing a standard for chain of custody it is critical that the standard incorporates all stakeholders in the tape management life-cycle and that no change in custody goes unrecorded.

All enterprises should also consider locking the chain of custody database so that it cannot be manipulated from outside the asset management software. It is highly recommended that the following enterprises require that the chain of custody record cannot be retrospectively modified:

- Enterprises which operate under Freedom of Information laws such as policing.
- Enterprises with a high security requirement such as defence and intelligence.
- Enterprises with a high chance of litigation such as healthcare and pharmaceutical.
- Enterprises with a high degree of regulation such as transport and financial services.
- Enterprises under strict Corporate Governance laws such as publicly listed corporations.

Chain of Custody Standards

- That every change in physical location of a tape be recorded.
- That any data which influences the location of a tape, such an expiry or move date be recorded and that any change to this data also is recorded.
- That changes to a chain of custody record can only occur through the asset management

software and that where third party modifications are required that this can only occur though an Application Programming Interface (API) call.
- That for a change in the chain of custody to occur a user must be authenticated and securely logged on.
- That the User-ID, date, time, location and interface of the updating user be recorded for each update that changes the location or may influence the location of a tape in the future.
- That chain of custody events exist for acquisition, usage, movement,decommissioning and destruction of each tape volume.
- That regular automated audits are run comparing known information and looking for discrepancies within the chain of custody.

Chain of Custody KPIs

- Number of chain of custody events being captured per stakeholder.
- Number of atypical chain of custody events recognised and recorded.
- Number of individual audit failures.
- Number of chain of custody changes that occur outside the asset management system (when allowed).

---

[1]HIPPA (USA), Sarbanes-Oxley (USA), Data Protection Act (UK)
[2]Linnen V Robins(http://cyber.law.harvard.edu/digitaldiscovery/digdisc_library_9.html)