

ADOPTED EDEN Standard No. 4

CHAIN OF CUSTODY

EDEN members maintain strict, documented chain of custody protocols to ensure the integrity of evidence placed under their control.

Please submit comments, suggestions, and inquiries to: standards@edenhub.com.

COMMENTARY

EDEN members providing electronic discovery services must implement and enforce comprehensive protocols for maintaining and documenting chain of custody for every evidence item under their control. This includes both the original evidence items as well as the data extracted from them, and includes all aspects of e-discovery, from initial data collection to production and storage.

Although the need for strict chain of custody controls is most often identified with criminal proceedings, the risks of improper chain of custody controls apply with equal force to e-discovery in support of civil litigation. In all cases, maintaining documented chain of custody protocols is of particular importance where electronic evidence is concerned, as electronic data is inherently fragile and readily subject to accidental or intentional alteration, corruption, or other manipulations that are often undetectable and irreversible if performed by experienced computer technicians.

In light of the malleable nature of electronic data, e-discovery chain of custody involves more than just documentation of the transfer of evidence between parties. The ability to establish with reasonable certainty what has *not* been done to electronic evidence is as important as reliable documentation of what has been done. Accordingly, chain of custody protocols must also address issues such as physical and virtual security. Concepts such as the storage of data sources in access-controlled environments and computer network security are critically important to maintaining the integrity and authenticity of evidence.

Without documented chain of custody protocols in place, e-discovery service providers and their clients risk facing unanswerable questions regarding the integrity of electronic evidence; questions that can diminish the impact or lead to outright exclusion of critical evidence at trial.

Given the diverse membership of EDEN, specific requirements for what is necessary to satisfy EDEN Standard No. 4 must be subject to the practical needs and realities of each individual member. For example, with regard to physical access control, whether

the appropriate level of security is a secure vault that is actively monitored on a 24/7 basis or a simple locked storage cabinet can only be answered on a case by case basis. What the Standard requires is that EDEN members proactively implement and consistently enforce a documented chain of custody program to minimize the risks to their clients of intentional and accidental data manipulation.

Please submit comments, suggestions, and inquiries to: standards@edenhub.com.

PROCESS SUPPORTING STANDARD

Successful chain of custody protocols must be grounded in form-based documentation. The consistent use of properly created and regularly revised forms minimizes the risk of error that is inherent in reliance on fallible human memory, unstructured technician note-taking, and other informal methods.

Forms developed in advance and informed by practical experience can serve as a helpful guide to technicians engaged in data extraction under the pressures of the field, ensuring that important details are not overlooked.

A model Electronic Evidence Custody Record supporting Proposed EDEN Standard No. 4 is available to EDEN members for review and comment in the member portal at: <http://edenhub.com/resourcesMem.html>. Used properly, the model Electronic Evidence Custody Record serves as reliable documentation of the transfer of custody of evidence between parties, as well as a log of every activity, from processing to production, to which the evidence is subjected.

Together with individual process logs documenting specific actions taken, such as the EDEN Hard Drive Cloning Log, the Electronic Evidence Custody Record provides a concrete base for testimony regarding data authenticity and integrity should questions arise. A copy of this form should be completed for each data-storing evidence item and should be provided to clients and preserved in internal files for future reference.



EDEN members are a diverse group, and although EDEN makes every effort to develop model forms that are useful in a broad range of contexts, members are reminded that the EDEN forms are examples intended for a broad audience that should be tailored as necessary to individual needs and practices.

Please submit comments, suggestions, and inquiries to: standards@edenhub.com.