

A Guide to the Creation of a Data Retention Policy

A data retention policy is a recognized and proven protocol within an organization for retaining information for operational use while ensuring adherence to the laws and regulations concerning them. The objectives of a data retention policy are to keep important information for future use or reference, to organize information so it can be searched and accessed at a later date and to dispose of information that is no longer needed.

The data retention policies within an organization are a set of guidelines that describes which data will be archived, how long it will be kept, what happens to the data at the end of the retention period (archive or destroy) and other factors concerning the retention of the data.

A part of any effective data retention policy is the permanent deletion of the retained data; achieving secure deletion of data by encrypting the data when stored, and then deleting the encryption key after a specified retention period. Thus, effectively deleting the data object and its copies stored in online and offline locations.

Lawful Intercept Standards

To ensure industry-wide implementation of the assistance capability requirements of Section 103 of CALEA, the FBI, through its CALEA Implementation Unit (CIU), in coordination with other federal, state, and local law enforcement agencies, consults with the appropriate standards-setting organizations of the telecommunications industry. The information listed below represents the lawfully-authorized electronic surveillance technical standards and specifications published by United States-based standard-setting organizations and industry associations of which the CIU is aware, cross-referenced against the various types of telecommunications services to which the standard or specification relates. The listed standards and specifications are available to the public on the referenced organization and association Internet websites. The list is provided for reference only and is subject to change as additional standards are developed and published.

Specifications can be purchased from ATIS.

**Lawfully Authorized Electronic Surveillance (LAES) For Internet Access and Services
ATIS -1000013.a.2007. Use Supplement A to ATIS-1000013.a.2009 in conjunction with
ATIS-1000013.2007**

<https://www.atis.org/docstore/default.aspx>