

# Technology Committee E-Filing Guidelines

Adopted by the Technology Committee on August 8, 2007

Adopted by the Judicial Council on September 25, 2007

---

## Recommendations:

- Create a multi-vendor electronic filing system
- Create a vendor certification process to ensure compliance with Utah court filing procedures
- Adopt standards to guide the electronic filing process
- Create a certifiable and accessible electronic court record.

## Standards:

### Document filing

Any document submitted to the court's electronic filing system must be submitted in a *searchable* PDF format. The sub-committee also recommends that the filer be responsible for the conversion of documents to the PDF format prior to filing.

### Electronic case record

The current rule requiring the filer to retain the original document should remain intact. Documents filed through the electronic filing system should be stored as submitted, without alteration, in the court's document management system.

### Electronic document validation

The Utah courts should contractually require each electronic filing service provider to authenticate the identity of the filer. Documents filed with the court should be digitally certified by the court when filed. Documents retrieved from the court's computing system should be authenticated when presented to the user.

### Electronic document retrieval

All parties to a case should be allowed to retrieve and view all documents relating to that case. Xchange should be modified to allow subscribers to access documents directly from Xchange through the case history screen. The subscription rate for Xchange should be reviewed to reflect the new capability of document retrieval and printing. The allocation of Xchange subscription revenue should be modified to account for the loss of copy fee revenue in the courts. The AOC should create a portal for individuals to validate documents on a known case without having to subscribe to Xchange.

### Electronic notice

When the court's electronic filing system initiates a service message, the agreement with the electronic service provider should require a response from the provider that the service message has been received and delivered to the intended recipient. Recording and storing the provider's receipt of the message would constitute a valid service. This process should not replace the requirement for the filing of a return of service document.

## **Filing Date**

For purposes of electronic filing, the file date will be the date and time recorded when the document has passed the initial document validation edits and is posted to clerk review by the electronic filing manager.

## **Technical failure**

The filer is responsible for a timely filing and should take appropriate action if the electronic filing system failed to notify the filer of the receipt of a filing action.

## **Protect confidential information**

It is the sole responsibility of counsel and the parties to redact personal identifiers that is visible within the body of an electronically filed document. Court clerks will not review any e-filed document to determine whether it includes personal information. Personal information not protected will be available through Xchange.

Filers should carefully review proposed pleadings and attachments with regard to the inclusion of personal information. Certain types of sensitive information should not be displayed in documents filed with the Court. If sensitive information must be included, the personal data identifiers should be redacted in the document.

- a. Social Security numbers - show only the last four numbers;
- b. Names of minor children - show only the initials;
- c. Dates of birth - show only the year;
- d. Financial account numbers - show only the last four numbers; and
- e. Home addresses - show only the city and state.

In addition, counsel shall carefully consider whether the following types of information should be redacted in a court filing:

- f. Personal identifying numbers such as driver license number;
- g. Medical records including treatment and diagnosis records;
- h. Employment history;
- i. Proprietary or trade secret information;
- j. Information regarding an individual's cooperation with the government; and
- a. Information regarding the victim of criminal activity.