

# Standards and Best Practices for Electronic Court Proceedings

November 2020

This document provides detailed specifications for Electronic Court Proceedings (ECPs) that utilize remote appearance technology. The focus of the standards and best practices is to meet the court's needs for operating and managing ECPs in advancing the effectiveness and efficiency of the judicial process.

Florida courts that are authorized or required to conduct ECPs by remote appearance technology shall comply with the following minimum requirements. "Standards" are intended to be mandatory practices that must be implemented. "Best Practices" are suggested practices intended to improve operations, but due to the court's platform or other local conditions, may be modified if necessary.

## *ECP Requirements*

### 1) Platform for ECPs

The hardware, software, and network architecture collectively comprise the "platform" for conducting ECPs. The platform shall be able to support court proceedings by videoconference, but these standards do not limit the court's discretion to hold court proceedings by telephone or other audio-only means.

#### *Platform Standards*

- Be accessible to all participants using equipment and software widely available and inexpensive or free from the user standpoint;
- Support multiple party, two-way audio and video communication, affording all participants the ability to see and be seen, to hear and be heard, and to see and hear every part of the ECP the judge sees or hears;
- Support an option to appear by telephone or other voice-only means for participants;
- Support the ability to share documents on the screen, unless the court has a different system for sharing documents;
- Enable public observers to see and hear every part of the ECP that the judge sees or hears;
- Enable the court or its designee to control access to an ECP, mute and eject disruptive attendees when necessary, and have the ability to disable screen-sharing;
- Use reasonable network protocols and strong encryption as required in the security standard section of this document; and
- Use reasonable error-handling procedures. In particular, notifying participants when the court becomes disconnected from an ECP or passing controls over to court personnel, as the court directs.

### *Platform Best Practices*

The chief judge should consider the extent to which it is feasible and desirable to implement uniformity in ECP platforms within the court and should consider whether to issue an administrative order addressing implementation of ECP platforms consistent with these standards. For the trial courts, uniformity may be within the circuit or within each county in the circuit. The choice of ECP platforms should be guided by:

- Maximizing effectiveness for ECPs;
- Ease of use;
- Integration with existing systems;
- Attention to security needs;
- Availability of understandable instructional materials;
- Exclusion of participation fees for utilizing the ECP platform; and
- A reasonable privacy policy.

## 2) Notification of Electronic Court Proceedings

### *Notification Standards*

- The notice must comply with the same criteria that would apply if the proceeding were in-person;
- The notice must ensure that it identifies the platform to be used and contains the information necessary to gain electronic entry to the ECP or instructions for obtaining that information;
- The notice must contain information that would allow a member of the public to observe the ECP, except in cases or proceedings made confidential by law;
- The notice must be placed in the court file; and
- The notice must advise of the applicable court personnel for receiving and responding to requests for accommodation under the Americans with Disabilities Act (ADA).

### *Notification Best Practices*

- Trial courts should consider formulating a standard Notice of Hearing for ECP events in each division within a circuit or a county within the circuit;
- The notice should contain the following expectations for participants attending ECPs:
  - Test equipment and connection ten minutes before the ECP starts;

- Reduce or eliminate background noise;
- Properly identify participants at the beginning of the ECP:
  - If attending via the videoconference function, participants should ensure that their name and role in the ECP (e.g. counsel for plaintiff, assistant state attorney, assistant public defender, or witness) is reflected in the user's identification.
  - If attending by telephone, where possible the participant should announce their appearance to allow the court and court reporter to correlate the phone number with their identity.
- Refrain from consuming food during the ECP;
- Mute the session unless speaking;
- Wear proper attire;
- Raise a virtual hand before unmuting unless directly spoken to;
- Do not speak over another participant unless making a lawful objection;
- Be aware and alert of surroundings that might create background noise or a lack of privacy relating to sensitive discussions;
- Turn off or mute other electronic devices that may create interruptions or distractions (e.g., mobile phones or notification settings with audible alerts); and
- Avoid "backlighting" by having a light source emanating from the direction of the screen and camera towards the participant.
- When the notice does not contain the information, the court should publish its expectations in a manner accessible to ECP participants.

### 3) Conduct of Electronic Court Proceedings

#### *Conduct Standards*

- The judge or judge's designee shall fulfill the role of host, or the judge may also designate co-hosts or alternative hosts;
- The judge or judge's designee is responsible for controlling the attendance and decorum of the ECP as a "virtual bailiff";

- The virtual bailiff shall provide for orderly resumption or termination of the ECP if the proceeding is disconnected;
- The virtual bailiff shall be able to perform the following functions, if available on the platform and as directed by the judge:
  - Set host and user permissions as described in the Recommended User Permissions Table attached as [Appendix A](#);
  - Implement a waiting room or lobby that attendees join before they are admitted into the ECP; and
  - Manage the waiting room, ensure that attendees in the waiting room are identified by name and role in the case, and admit attendees into the ECP;
  - Request that attendees identify themselves in the online platform using their full name and who they represent;
  - Admit only authorized attendees, where discernable, and keep other participants out of the ECP until their presence is required;
  - Remove unruly attendees;
  - Turn off screen-sharing by default, unless temporarily opened to allow a participant to display screen details;
  - Disable all chats or make the feature available only to the host/co-host;
  - Use a mechanism or procedure to prevent a removed participant from returning;
  - Set the ECP to contain a password requirement to reduce the possibility of unauthorized individuals commandeering the ECP;
  - Identify any removed unruly participants and, when appropriate, report them for potential investigation or prosecution;
  - Configure ECPs where microphones are muted upon entry for all participants;
  - Permit access to private conversation rooms to allow attorneys and their clients to discuss privileged matters, to sequester witnesses, or to hold sidebar discussions in public ECPs;
  - Start live streaming; and
  - End the ECP for all participants.

### *Conduct Best Practices*

- The virtual bailiff should remind participants of the ECP decorum expectations, and enforce those expectations if necessary; and
- The judge should determine whether to host the ECP themselves or delegate that function to court personnel, on a case-by-case basis.

## 4) Identification in ECPs

### *Identification Standards*

- The virtual bailiff shall require each of the participants in an ECP to identify themselves;
- All participants in an ECP must accurately identify themselves by first and last name, in addition to being prepared to show a driver's license or other identifying document if required; and
- When taking testimony or otherwise relying on the statements of a participant in an ECP, the court shall consider the level of risk of impersonation, the reliability of the witness's claims of identity, and require any additional proof of identity that the court deems necessary.

### *Identification Best Practices*

- When the risk of false identity or impersonation is low, the court should require a low level of proof of identity (e.g. - accepting a sworn or unsworn statement of identity or the representation by counsel that a person is whom the person claims to be); and
- When the risk of false identity or impersonation is higher, the court should require a higher level of proof of identity (e.g. - requiring the person to display identification documents over the platform). Other methods of gaining evidence of identity could include having the person call the court from a phone that identifies the person in its caller ID, asking the person for a phone number at which they can be called, or requiring the person to respond to their email address on file with the court or the Florida Courts E-Filing Portal, if either exists.

## 5) Attendance in ECPs

Occasionally, there may be persons who intend to be present in a certain ECP, but who inadvertently end up attending the wrong proceeding.

### *Attendance Standards*

- The court should take reasonable measures to prevent or mitigate detriment or harm resulting from a participant inadvertently appearing or remaining in the wrong ECP.

### *Attendance Best Practices*

- When feasible, at the beginning of each ECP the judge or virtual bailiff should announce the name of the judge, type of docket, and name of each case being addressed; and
- The court should consider maintaining a master calendar of ECPs, for reference purposes, if resources permit.

## 6) Public Observation in ECPs

### *Public Observation Standards*

- Except for cases or proceedings that are confidential pursuant to law, the court must allow for ECPs to be open for public observation; and
- Participants in an ECP must be made aware that the ECPs are public proceedings. When the case or proceeding is not confidential by law in its entirety, but a participant asserts that some aspect of it is entitled to be treated as confidential, the participant must raise the matter to the court for appropriate action.

### *Public Observation Best Practices*

- Openness to the public may be accomplished by:
  - Live streaming on a widely available streaming service; and
  - Use of a "webinar" feature, if available in the platform, to allow for the admission of participants (sometimes called "panelists") and observers separately, and to allow blocking participation by observers.

## 7) Sensitive Information in ECPs

### *Sensitive Information Standards*

- For cases or proceedings that are confidential pursuant to law, the court must preserve confidentiality during ECPs using the highest levels of security as described in the security section of this document; and
- For other cases or proceedings, any claims of confidentiality of information must be resolved by the court on a case-by-case basis, and information the court finds confidential shall be protected as described in the security section of this document.

### *Sensitive Information Best Practices*

- Platforms that have a feature for assigning users to private groups ("breakout rooms") should be utilized for off-the-record discussions, sequestration of witnesses, *in camera* inspections, and other nonpublic matters.

## 8) Security in ECPs

The principal security risks of ECPs are intrusion and interruption, and for cases, proceedings, and information that are confidential pursuant to law, unauthorized interception is prohibited. The most effective way to minimize the risk of third-party interruptions is to configure the platform's settings before or during an ECP. Recommended security control settings are included as a guide in managing ECPs ([see Appendix B](#)).

### *Security Standards*

- The court or designated court personnel shall be able to implement the following security measures, as directed by the court:
  - "Waiting room" or other holding area where persons seeking admission to an ECP can be (virtually) placed until the court is ready for them;
  - Passcodes specific to the ECP;
  - Lock an ECP once all participants are present;
  - Remove disruptive participants;
  - Readmit a removed participant;
  - Disable the audio and video feeds from all participants at once;
  - Disable or enable file transfer functions;
  - Disable or enable annotations or chat features;

- Disable or enable screen sharing;
- Start or stop any recording by the platform; and
- Report abusive participants to the appropriate authorities.
- Cryptographic security in all ECP platforms must:
  - Be protected by end-to-end encryption;
  - Employ a hosting service that has a valid Secure Sockets Layer (“SSL”) certification in place; and
  - Activate connection throttling to minimize the risk of a distributed denial-of-service attack.

#### *Security Best Practices*

- Waiting rooms and/or passcodes should be on by default or set to on in each ECP; and
- Screen sharing, file upload, annotations, and chat features should be disabled by default.

### 9) Recording in Electronic Court Proceedings

A judge should review the circuit-wide plan or administrative order for the court reporting or electronic recording of any judicial proceedings (see Rule 2.535 of the Florida Rules of Judicial Administration).

#### *Recording Standards*

- The judge or virtual bailiff should provide notice to ECP participants that the proceeding may be recorded; and
- Participants are not authorized to make their own recordings of the ECP.

#### *Recording Best Practices*

- ECP recordings should be stored on a local machine rather than in the cloud or other storage system.



## 10) Integration in ECPs

### *Integration Standards*

- When choosing a platform, courts shall consider the degree to which a platform is able to integrate with existing or potential systems for digital court reporting, virtual remote interpreting, and other court technology systems.

### *Integration Best Practices*

- Video conference platforms should be able to integrate with digital court reporting, virtual remote interpreting, and other court technology systems, using industry standard protocols and application programming interfaces (APIs).

## 11) ADA in Electronic Court Proceedings

### *ADA Standards*

- ECPs must comply with the ADA requirements.

### *ADA Best Practices*

- All video platform solutions should comply with the ADA requirements and courts should be mindful of this goal in evaluating various platforms;
- The Web Content Accessibility Guidelines (WCAG) 2.0 Level AA is the criteria used to gauge whether electronic state and local government platforms such as websites are accessible; and
- In determining whether a particular platform is accessible to users with disabilities, information may need to be obtained from the platform provider to determine what steps the platform has taken to address accessibility, including the platform's compliance with WCAG 2.0.

## Appendix A – Recommended User Permissions

Features with an asterisk (\*) can be enabled or disabled by the host during the meeting.

Feature	Host	Co-host/ Alternative host	Participants
<b>Participating in the meeting</b>			
Start the meeting	✓	<a href="#">see note</a>	
Mute/unmute themselves*	✓	✓	✓
Start/stop their own video	✓	✓	✓ *
View participants list	✓	✓	✓
<a href="#">Share screen</a>	✓	✓	✓ *
<a href="#">Request or give remote control</a>	✓	✓	✓
Chat with participants ( <a href="#">in-meeting chat</a> )	✓	✓	✓
Save <a href="#">in-meeting chat</a>	✓	✓	
Create or edit <a href="#">polls</a>	✓		
Start <a href="#">polling</a>	✓	✓	
Answer <a href="#">polls</a>			✓
Assign someone to enter <a href="#">closed captions</a>	✓		
Enter <a href="#">closed captions</a>	✓	✓ *	✓ *

<b>Feature</b>	<b>Host</b>	<b>Co-host/ Alternative host</b>	<b>Participants</b>
End meeting	✓		
<a href="#">Reactions</a> and <a href="#">nonverbal feedback</a>	✓	✓	✓
<a href="#">Managing participants</a>			
Mute or unmute participants	✓	✓	
Stop participant's video	✓	✓	
Ask participant to start video	✓	✓	
<a href="#">Spotlight a video</a>	✓	✓	
Promote participant to host or co-host	✓		
Change who attendees can chat with	✓	✓	
Remove attendees	✓	✓	
Put participants on hold	✓	✓	
Rename participants	✓	✓	
<a href="#">Invite others</a> to join	✓	✓	✓
Mute controls for participants (ask to mute, mute all, mute on entry)	✓	✓	

Feature	Host	Co-host/ Alternative host	Participants
Assign participants to <a href="#">breakout rooms</a>	✓		
<b>Recording</b>			
Start <a href="#">cloud recording (if applicable)</a>	✓	✓	
Start <a href="#">local recording</a>	✓	✓	
Allow or forbid a participant to start local recording	✓	✓	
<b>Live streaming</b>			
<a href="#">Live stream on Facebook</a>	✓		
<a href="#">Live stream on Workplace</a>	✓		
<a href="#">Live stream on YouTube</a>	✓		
<a href="#">Custom live stream</a>	✓		

## Appendix B – Recommended Security Control Settings\*

*\*Some settings are not available on all platforms.*

### **Pre-meeting:**

- Waiting Room: Enabled
- Passcodes: As needed

### **In Meeting:**

- Lock meeting: Enabled
- Passwords: As needed
- Manage Participants
  - Remove
  - Hold
  - Disable video
  - Mute
- File Transfer: Disable
- Annotation: Disable
- Private Chat: Disable
- Screen Sharing: Restricted to host and/or Co-host

### **Platform Infrastructure:**

- Valid SSL Certificate
- Encryption
  - In transit: End-to-End over TLS 1.2 (or higher) connection
  - At rest: AES 256
  - Hashing: SHA 256
  - Connection Throttling: Enabled