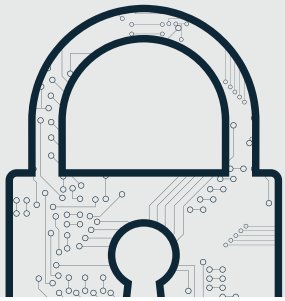
American Arbitration Association® | International Centre for Dispute Resolution®

AAA-ICDR® Best Practices Guide
for Maintaining Cybersecurity and Privacy



The AAA-ICDR is committed to the security and privacy of customer and case information. To effectuate that goal AAA-ICDR has implemented best practice policies, procedures and technologies internally to help protect its data and information systems. The protections that have been implemented apply to all case data and equipment stored and managed on the AAA-ICDR technology infrastructure. AAA® employees routinely participate in online training programs designed to heighten their knowledge of security policies and procedures. The AAA has also prepared a *AAA-ICDR Cybersecurity Checklist* which parties and/or their representatives as well as arbitrators may use as a resource.

Recognizing that cybersecurity is a shared responsibility, AAA-ICDR is requiring all arbitrators on its panels to complete a training course by year-end 2020. The program is designed to educate the arbitrators as to the cybersecurity basics so they can preserve and protect the integrity and legitimacy of the arbitral process in cases in which they are serving.

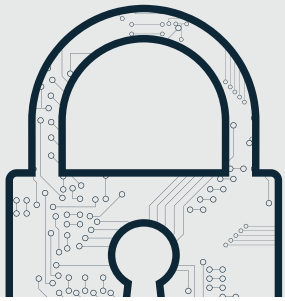
The level of cybersecurity that should be implemented during arbitration ultimately rests with the parties and their legal advisors. The American Bar Association has issued two opinions regarding a lawyer's obligations either after an electronic data breach or cyberattack (Formal Opinion 483) or when securing email communication of protected client information (Formal Opinion 477).

In accordance with the ABA guidance, legal counsel in consultation with their clients should assess the nature of the information to be shared during arbitration and the impact of a cybersecurity breach on their client's business. A risk assessment should be undertaken in which counsel and the client identify whether highly sensitive data, such as personal, classified, financial, commercial or confidential information, is pertinent to the dispute and whether a particular approach must be taken during the collection, storage and transmission of such data to opposing counsel, arbitral institutions and arbitrators. In a case with a heightened need for cybersecurity, parties may elect to screen prospective arbitrators by means of a cybersecurity checklist designed to identify potential security concerns.

The following best practices are designed to provide guidance to parties, their representatives, and arbitrators regarding cybersecurity measures they should consider adopting. It does not impose hard or fast rules, but rather encourages an in depth discussion of the potential risks and reasonable and proportionate protective measures that might be taken to better secure sensitive information. These best practices are not intended to ensure compliance with any applicable laws, regulations, professional or ethical obligations.

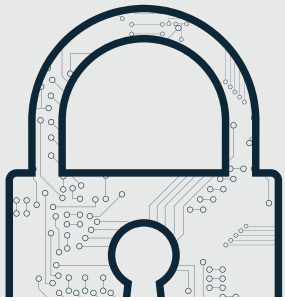
1. During the preliminary hearing, the parties and/or their representatives and arbitrator should discuss reasonable precautions to be taken with regard to cybersecurity, privacy, and data protection to ensure an appropriate level of security for the case.
2. Early in the proceeding, and no later than the preliminary hearing, the parties' representatives should also discuss whether they plan to exchange information that presents a heightened need for cybersecurity, such as confidential information or personal data.

AAA-ICDR® Best Practices Guide
for Maintaining Cybersecurity and Privacy



3. In connection with the above, arbitrator(s) and parties' representatives should discuss the following:
    a. Does this case require an enhanced level of cybersecurity, privacy or data protection? If yes, why?
    b. Is there confidential information that will require specific security practices and measures? If yes, how should these specific practices and measures be incorporated in this proceeding?
    c. How do participants plan to ensure that all case related email communications are secure? Are there any concerns with the security level of the email accounts or service providers being utilized by all participants?
    d. What electronic and/or hardcopies of hearing briefs or other related documents will be submitted in this proceeding? Who needs electronic versions? Who needs a flash drive? Must flash drives be encrypted with a password? Who needs hardcopies? What are the conditions under which an authorized recipient can further share a document?
    e. How do participants plan to ensure secure exchange and storage of electronic versions of case related documents and files?
        a. If the participants wish to use email, are they willing to use Citrix ShareFile for encrypted email transmission of case related documents? If yes, do you want AAA to provide instructions for use of Citrix ShareFile?
        b. Are all the participants willing to use AAA WebFile® and Panelist eCenter® in-lieu of email for all case related documents and/or storage? If yes, do you want AAA to provide instructions for use of AAA-ICDR WebFile? If no, do the parties require a different common secure cloud service for document exchange and storage?
    f. How do participants plan to ensure secure storage of all case related documents and files once exchanged? Is everyone satisfied with the secure storage measures currently being utilized by all participants?
    g. Do the parties plan to submit sensitive personal identifiers, including national identification numbers, dates of birth, medical health information, intellectual property, privileged information, credit card or financial account numbers, or other similar personal information? If yes, is it essential that this information be submitted? If it is essential, can the data be redacted?
    h. Will any third parties (companies or individuals) need access to any case related documents? If yes, who, why, what and how? Will additional security measures be necessary when submitting documents to third parties?
    i. When and how should case related documents be destroyed by the participants? Should there be written confirmation of document destruction by all participants and third parties?
    j. Will all participants and third parties agree to notify all participants of any security concerns, incidents, or breaches within 24 hours?
    k. Are there any other issues that need to be discussed relating to cybersecurity, privacy or data protection?

AAA-ICDR® Best Practices Guide
for Maintaining Cybersecurity and Privacy



4. Parties should identify any contractual obligations, such as confidentiality agreements, applicable laws or regulations governing information security.
5. A deadline should be set by the arbitrator for the parties to meet and agree upon procedures to govern the handling of sensitive information:
    a. Transmission of any and all sensitive communications by the parties, among arbitrators, between arbitrators and with any administering organization;
    b. Storage of arbitration-related sensitive information;
    c. Sharing of arbitration-related sensitive information with authorized third parties, such as arbitral participants, fact witnesses, experts or vendors, such as a stenographer.
    d. Breach detection and notification to all parties, the arbitrators, participants and, if applicable, government regulators.
    e. Retention and destruction of sensitive case documents.
6. The parties' agreement on the cybersecurity measures to be employed should be adopted by the arbitrator(s) unless the arbitrator(s) determine that applicable law requires additional security measures.
7. If the parties disagree as to the cybersecurity procedures that must be implemented, the arbitrators should provide the parties with an opportunity to address whether the measures are reasonable and proportionate prior to adjudication by the arbitrator and issuance of an order.
8. If a party objects to the continued service of an arbitrator due to an alleged inability to comply with the required cybersecurity measures either agreed to by the parties or ordered by the arbitrator(s), the issue may be submitted to AAA's Administrative Review Council.
9. A copy of the mandatory cybersecurity measures either agreed to by the parties or ordered by the arbitrator(s) should be provided to all participants and authorized third parties who will be required to confirm in writing that they are in compliance.
10. The arbitrator following discussions with the parties should determine what action should be taken if a participant is unable to comply with the cybersecurity requirements.