Ohio Court Security Standards

Appendix C

Sup.R. 9, Court Security Plans

Updated March 2025

Ohio Court Security Standards

Appendix C

Sup.R. 9, Court Security Plans

Sharon L. Kennedy

CHIEF JUSTICE

Patrick F. Fischer

R. Patrick DeWine

Jennifer Brunner

Joseph T. Deters

Daniel R. Hawkins

Megan E. Shanahan

JUSTICES

Robert W. Horner, III

ADMINISTRATIVE DIRECTOR

Office Of Court Security

Ryan J. Fahle
DIRECTOR OF COURT SECURITY

Christopher Luginbuhl
MANAGER OF COURT SECURITY

John A. Groom
SECURITY SERVICES MANAGER

AMENDMENTS TO THE RULES OF SUPERINTENDENCE FOR THE COURTS OF OHIO

The following amendments to the Rules of Superintendence for the Courts of Ohio (Sup.R. 9) were adopted by the Supreme Court of Ohio on Nov. 18, 2008, and become effective on March 1, 2009. The history of these amendments is as follows:

May 12, 2008	Initial publication for comment
Nov. 18, 2008	Final adoption by conference
March 1, 2009	Effective date of amendments

AMENDMENTS TO THE
RULES OF SUPERINTENDENCE FOR THE COURTS OF OHIO

***

Sup.R. 9. Court Security Plans.

(A) Court Security Plan

For purposes of ensuring security in court facilities, each court shall develop and implement a court security plan. If more than one court occupies a court facility, the courts shall collectively develop and implement a single court security plan. In addition to any other provisions necessary to satisfy the purposes of this rule, the plan shall address the provisions of the Ohio court security standards adopted by the Supreme Court and as set forth in Appendix C to this rule.

(B) Public Access

For purposes of ensuring security in court facilities, a court security plan, including any security policy and procedures manual, emergency preparedness manual, and continuity of operations manual adopted as part of the court security plan, shall not be available for public access.

Sup.R. 99. Effective Date

***

(ZZZZ) The amendments to Appendix C, adopted by the Supreme Court of Ohio on March 30, 2021, shall take effect on July 1, 2021.

***

PREAMBLE

The following Ohio Court Security Standards represent the efforts of the Supreme Court Advisory Committee on Court Security. The Standards were first adopted by the Supreme Court in 1994 and are now revised to reflect changes in our society affecting them.

Ohio citizens should expect all court facilities to be safe and secure for all who enter so that justice for all may be sought and not unjustly interrupted. Court facilities and each courtroom therein should have appropriate levels of security to address any foreseeable concern or emergency that may arise during the course of business. Elected officials charged with court facility authority must be proactive and sensitive to court security and emergency preparedness concerns. While the Advisory Committee understands providing a safe court facility to all carries a financial price, it is imperative that the topics discussed in the Ohio Court Security Standards be addressed.

Court security and emergency strategies and actions must be consistent with individual rights, civil liberties, and freedoms protected by the United States Constitution, the Ohio Constitution, and the rule of law. Because Ohio has a diverse population, special thought should be given to overcoming language and cultural barriers and physical disabilities when addressing security and emergency issues. However, Ohio citizens must be assured that any security practice or policy is employed in a neutral manner.

The Ohio Court Security Standards attempt to balance the diverse needs of each community. However, each locale is encouraged to promulgate policies and procedures to meet its specific needs. Special consideration should be given to defining the roles and responsibilities of the court and law enforcement officials within each local jurisdiction.


THE SUPREME COURT OF THE STATE OF OHIO

TABLE OF CONTENTS

STANDARD 1. COURT SECURITY COMMITTEE

Each court shall appoint a court security committee to meet on a periodic basis for the purpose of implementing these standards. If more than one court occupies a court facility, the courts shall collectively appoint a single committee.

Commentary

Court security issues affect many sectors of the community and include differing local needs and serious funding concerns. Therefore, a Court Security Committee should review these issues in a cooperative and constructive manner.

The Court Security Committee should include representatives of first responders, emergency management agencies, and funding authorities, and may include representatives from each entity within the court facility and the community.

STANDARD 2. SECURITY POLICY AND PROCEDURES MANUAL

(A) Adoption of manual

As part of its court security plan, each court shall adopt a written security policy and procedures manual governing security of the court and the court facility to ensure consistent, appropriate, and adequate security procedures. The manual shall include each of the following:

(1) A physical security plan;

(2) Routine security operations;

(3) An emergency action plan that addresses events such as a hostage situation, an escaped prisoner, violence in the courtroom, a bomb threat, and fire;

(4) A high risk trial plan.

(B) Review of manual

A court shall periodically test and update its security policy and procedures manual for operational effectiveness.

(C) Multiple courts

If more than one court occupies a court facility, the courts shall collectively adopt and review a single security policy and procedures manual.

Commentary

Although traditional forms of security, such as security searches of entrants to the court facility, are an excellent primary safeguard, it is important that courts have a written Security Policy and Procedures Manual addressing the items listed above.

To ensure a thorough knowledge of the court's Security Policy and Procedures Manual, all court security officers should review the manual as a part of their orientation and as a component of regular, continuing education for retained court security officers.

A copy of the Security Policy and Procedures Manual should be available to all court security officers to ensure they understand the appropriate security procedures.

All court security officers should be immediately informed of any changes or amendments to the Security Policy and Procedures Manual.

The Security Policy and Procedures Manual is a protected document which should not be shared with non-security court personnel other than court leadership. However, it is recommended that a shorter guidebook be prepared for all other court personnel, which should include emergency evacuation procedures, routes, and building safety guidelines.

STANDARD 3. EMERGENCY PREPAREDNESS MANUAL

(A) Adoption of manual

As part of its court security plan, each court shall adopt a written emergency preparedness manual. The manual shall include a plan providing for the safety of all persons present within the court facility during an emergency.

(B) Review of manual

A court shall periodically test and update its emergency preparedness manual for operational effectiveness.

(C) Multiple courts

If more than one court occupies a court facility, the courts shall collectively adopt and review a single emergency preparedness manual.

STANDARD 4. CONTINUITY OF OPERATIONS MANUAL

(A) Adoption of manual

As part of its court security plan, each court shall adopt a written continuity of operations manual. The manual shall include a plan that addresses each of the following:

(1) The continued operation of the court at an alternative site should its present site be rendered inoperable due to a natural disaster, act of terrorism, security breach within the building, or other unforeseen event;

(2) The provisions of the "Court Continuity of Operations (COOP) Plan Template" available on the website of the Supreme Court.

(B) Review of manual

A court shall periodically test and update its continuity of operations manual for operational effectiveness.

(C) Multiple courts

If more than one court occupies a court facility, the courts shall collectively adopt and review a single continuity of operations manual.

STANDARD 5. PERSONS SUBJECT TO A SECURITY SEARCH

All persons entering a court facility shall be subject to a security search. A security search should occur for each visit to the court facility, regardless of the purpose or the hour.

Commentary

The credibility of court security requires the public be subject to a security search when entering a court facility. Any exemption of personnel from the security search process, including elected officials, court personnel, attorneys, law enforcement officers, or court security officers, should be decided and documented by the Court Security Committee.

At a minimum, each court facility should have at least one portable walk-through magnetometer and a hand-held magnetometer, with court security officers trained in the proper use of that equipment. Walk-through magnetometers at a single point of entry, with accompanying x-ray viewing of packages and handbags, is the optimal method of searching entrants to a court facility and should be utilized to provide the type of security needed to ensure a safe environment. A single point of entry for the public is strongly recommended.

STANDARD 6. COURT SECURITY OFFICERS

(A) Assignment

Uniformed court security officers should be assigned in sufficient numbers to ensure the security of each courtroom and the court facility.

(B) Certification and training

All court security should be certified through the Ohio Peace Officers Training Council. These officers should receive specific training on court security and weapons instruction specific to the court setting.

Commentary

For the purpose of these standards, "court security officer" means an individual employed or contracted to perform security duties or functions at a court facility and includes a law enforcement officer assigned to court security and a bailiff who performs court security duties or functions. "Court security officer" does not include an administrative bailiff who does not perform court security duties or functions.

Law enforcement officers who are present within the court facility for purposes other than court security, such as testifying at a trial, should not be considered a component of the court security system. These law enforcement officers' full attention should be directed to the duties to which they are assigned. The security of the court should not be reliant upon these law enforcement officers, who may have no specific training in court security.

STANDARD 7. WEAPONS IN COURT FACILITIES

(A) Prohibition

No weapons should be permitted in a court facility except those carried by court security officers or as permitted under division (B)(1) of this standard. The court should establish and install adequate security measures to ensure no one will be armed with any weapon in the court facility.

(B) Law enforcement

(1) Each court should promulgate a local court rule governing the carrying of weapons into the court facility by law enforcement officers who are not a component of court security and are acting within the scope of their employment. If more than one court occupies a court facility, the courts shall collectively promulgate a single rule.

(2) In all cases, law enforcement officers who are parties to a judicial proceeding as a plaintiff, defendant, witness, or interested party outside of the scope of their employment should not be permitted to bring weapons into the court facility.

Commentary

There is no issue more controversial relating to court security than whether law enforcement officers should be required to surrender their weapons at the court facility door. As a result, each individual court should review its needs and formulate policy based upon local needs and realities.

STANDARD 8. PRISONER TRANSPORT WITHIN COURT FACILITIES

(A) Transport

Prisoners should be transported into and within a court facility through areas that are not accessible to the public. When a separate entrance is not available and public hallways must be utilized, prisoners should be handcuffed behind the back or handcuffed with use of "belly chains" to limit hand movement and always secured by leg restraints.

(B) Carrying of firearms

During the transport of prisoners, personnel in direct contact with the prisoners should not carry firearms. However, an armed court security officer should be present.

(C) Holding area

Once within a court facility, prisoners should be held in a secure holding area equipped with video monitoring, where practicable, while awaiting court hearings and during any recess.

Commentary

If prisoners cannot be transported through private court facility entrances, public movement in the area should be restricted during the time of prisoner transport since transport through a public area exposes the public to danger, enhances the possibility of prisoner escape, and increases the ability to transfer weapons or other contraband to prisoners.

Law enforcement officers should accompany prisoners to the courtroom, remain during the hearing, and return prisoners to the secured holding area. Court security officers should not assume this responsibility.

STANDARD 9. DURESS ALARMS FOR JUDGES AND COURT PERSONNEL

All courtrooms, hearing rooms, judges' chambers, clerks of courts' offices, and reception areas should be equipped with a duress alarm system connected to a central security station. The duress alarm system should include enunciation capability.

Commentary

There are times when individuals may be able to circumvent standard court security measures. Judges and court personnel should have a readily accessible signal system upon which to rely in emergency situations.

It is important that the duress alarm system be a type which includes an audible alarm at the central security station. However, the system should not include an audible alarm at the activation site. The duress alarm system should quickly summon additional help from the county sheriff's office or the nearest police jurisdiction when needed.

To ensure confidence in the duress alarm system is maintained, duress alarms should be tested periodically and all efforts should be made to minimize false alarms.

STANDARD 10. CLOSED-CIRCUIT VIDEO SURVEILLANCE

If a court utilizes closed-circuit video surveillance, the system should include the court facility parking area, entrance to the court facility, court lobby, courtroom, and all other public areas of the court facility.

Commentary

Posted notices that every judicial proceeding is under surveillance may dissuade those who have intentions of disrupting a hearing. Some court facilities may lack the architectural and structural elements necessary for court security and, therefore, require greater reliance on security devices. Closed-circuit video surveillance is secondary to security searches of entrants to a court facility.

STANDARD 11. RESTRICTED ACCESS TO OFFICES

To ensure safe and secure work areas and to protect against inappropriate interaction between judges and participants in the judicial process, an effective secondary security perimeter should be utilized at the entrance to the office space housing judges and court personnel.

Commentary

The security of the office space housing judges and court personnel must be maintained. Unlimited access to these areas is dangerous and unnecessary. The general public should not be permitted to wander through these areas for any reason. However, attorneys should have controlled access to the areas. Persons having business with a judge or court personnel should be encouraged to make appointments.

Steps which may be taken to facilitate this standard include a main receptionist checkpoint, passive or active electromagnetic hall locks, and cardreader door locks.

Also, the judges' chambers, as differentiated from the staff offices, and judges' parking spaces should not be designated by "Judge" signage.

Finally, parking spaces should be located as close as possible to an entrance.

STANDARD 12. OFF-SITE PERSONAL SECURITY

As part of its court security plan, each court, in conjunction with law enforcement officers, should adopt procedures for the personal security of judges and court personnel at locations outside the court facility. If more than one court occupies a court facility, the courts shall collectively adopt procedures applicable to all judges and court personnel in the court facility.

Commentary

The protection of judges and court personnel from work-related threats and acts of violence outside the court facility is important. It is essential that procedures be in place, when necessary, to respond to such incidents.

The particular procedures may include personal security profiles, residential alarm systems, cellular telephones, weapons training, self-defense training, and personal/family bodyguard security. While all of these steps include some financial commitment, the procedures may be graduated to respond to the needs of any given situation.

STANDARD 13. STRUCTURAL DESIGN OF COURT FACILITIES AND COURTROOMS

When designing new or remodeling old court facilities, consideration should be given to circulation patterns that govern the movement of people to, from, and in the courtroom. Judges, juries, court personnel, and prisoners should have routes to and from the courtroom separate from public routes. Waiting areas should be available to allow separation of parties, victims, and witnesses.

Commentary

The circulation patterns should separate the prisoners from all other persons. The public should also be separated from the judges, juries, and court personnel.

STANDARD 14. SECURITY INCIDENT REPORTING

(A) Reporting of security incidents

(1) Every violation of law that occurs within a court facility should be reported to the law enforcement agency having jurisdiction. To facilitate reporting, all court personnel should familiarize themselves with the law enforcement agency that has jurisdiction within and around their court facility.

(2) Each court should adopt a policy for reporting court security incidents and should include the policy in the court's security policy and procedures manual. If more than one court occupies a court facility, the courts shall collectively adopt a single policy.

(3) A summary of court security incidents should be compiled annually for the court's benefit in evaluating security measures.

(B) Periodic review of security incidents

All courts within the court facility should periodically review all court security incidents so the judges and court personnel are aware of recent events.

Commentary

Although the facility may be a county court facility, in some areas, if the facility is located within the limits of a municipal corporation, the local police may be the law enforcement agency having jurisdiction.

A "court security incident" is any infraction outlined within the court's Security Policy and Procedures Manual and includes any and all disruptions made in the confines of the court facility.

To measure the effectiveness of court security procedures and to aid in securing necessary funding for court security measures, it is useful to recognize and record court security incidents. A standard incident reporting form should be utilized by court personnel to record each event which compromised the security of the court and/or the safety of the participants in the judicial process. Additionally, each court should do an annual summary of court security incidents for its own benefit in evaluating court security measures using the model incident reporting form.

STANDARD 15. COMMUNICATION DEVICES IN THE COURT FACILITY

The court security committee, along with other court officials, should consider and formulate a plan that governs the presence and use of communication devices in the courthouse, courtroom, and surrounding courthouse grounds. "Communication device" means any device intended to communicate, disperse, or retrieve information, including cell phones, computers, tablet computers, and cameras. The plan should comply with the requirements of Rule 12 of the Rules of Superintendence for the Courts of Ohio and provide all of the following:

(A) The use of communication devices in the courtroom, as well as the entrance into and departure from the courtroom, should be minimally intrusive so as not to disturb court functions or distract the court proceedings in any manner;

(B) Communication devices should be used and moved into and out of the courtroom safely, so as to protect all persons in the courtroom and not create an impediment to court operations;

(C) Except as provided in paragraphs (D) and (E) of this standard, at no time should the public, jurors, or witnesses be permitted to use communication devices in the courtroom. The plan should explicitly prohibit the public, jurors, and witnesses from using any communication devices while in attendance at trial. "Use" includes texting, audio and video recording, and still photography.

(D) If the court determines there is a need for such use, the court may permit the use of communication devices in the courtroom for scheduling purposes and to obtain or disseminate information. Other uses of communication devices in the courtroom should be at the court's discretion. Communication devices should either be turned off or put in silent mode when not in use.

(E) With the court's prior approval, the news media must be permitted to use communication devices in the courtroom. However, the plan should provide that no audio recording, video, or photograph of any juror, witness, or juvenile defendant should be taken.

(F) Appropriate signage should be posted identifying the procedure for use of communication devices in the courtroom and stating that use of communication devices in the courtroom may be prohibited if it interferes with the administration of justice, poses a threat to safety or security, or compromises the integrity of the proceedings.

Commentary

The presence of communication devices in the courtroom during court operations should be pre-approved to avoid disruption of court proceedings.

The use of communication devices for texting, audio/video recording, and still photography, has been a rather controversial subject resulting in varied responses from the courts. As a result, each court should adopt a Best Practices policy based on local court expectations and the ability to enforce its policy. Failure to comply with established Best Practices may result in a fine, including confiscation, incarceration, or both, for contempt of court.

STANDARD 16. INFORMATION TECHNOLOGY OPERATIONS SECURITY

With the proliferation of court information technology standards, each court should periodically evaluate and update its security for its information technology systems and operations. Information technology security is a broad and complex arena and this standard is best addressed by having a discussion with the court information technology representative and ensuring that these issues are understood. An adequate information technology security plan should include at least the following components:

(A) Disaster recovery

A disaster recovery plan is one of the most important aspects of every information technology security program. A disaster recovery plan, also known as a business continuity plan, can be defined as a set of steps an entity will take to get its business up and running in the event of a disaster.

(B) Physical security

Physical security addresses where key information technology equipment, such as servers, core routers and switches, and data storage, is housed and who has access to it. A well-designed server room should have access control restrictions. Only the people who need to be in the server room should have access to it. There should be humidity and temperature control in the room, as well as protection systems for smoke, fire, and water. Since server rooms tend to house critical equipment, backup emergency power, such as an uninterrupted power source or generator, should be considered.

(C) Patch management

Patch management involves keeping computer system firmware and software up to date. It is one of the most difficult administrative tasks for information technology professionals. New vulnerabilities are found every day. Keeping all systems up to date on patches and fixes can take much time and effort, but can also provide the greatest benefit in terms of security threats.

(D) Endpoint/antivirus security

A comprehensive endpoint antivirus security solution should be used on all network attached computers to prevent malware infections on user devices. Antivirus software must frequently be updated in order to protect against the ever-growing list of threats. A good antivirus product will be one that can be automatically updated on a daily basis with new threat detection files.

(E) Access control security

Access control involves managing who has access to different resources. The principle of least privilege for users, groups, and applications should be used. This principle involves restricting access for users, groups, and applications to only those required to perform the job.

(F) Authentication and authorization

Authentication is the use of security methods and processes such as identification and passwords to verify the identity of a user. Authorization is the process of checking whether a person, an information technology component, or an application is authorized to perform a specific action.

(G) Network security

Network security can involve a wide range of tools and methods to help secure the information technology systems. At a minimum, the information technology security plan should include both of the following components:

(1) A firewall, which is a system or set of systems that control access between the internal network and some other external network, such as the internet. A firewall is a gateway to the network that controls access. Firewalls provide the first line of defense for network security infrastructure. The firewall protection methods may include access control lists, blacklists, VPNs, proxy/NAT, etc.

(2) Access control lists on network routers and switches. An access control list is an ordered set of rules that is used on routers and switches to filter traffic. Access control lists are used to protect networks and specific hosts from unnecessary or unwanted traffic. For example, access control lists can be used to disallow internet traffic from a high-security network to the internet.

(H) Email security and protection

Email security appliances and software, such as spam filters, should be used to protect against phishing and virus emails and to keep unwanted email from entering your users' inboxes and junk folders. Users also should be taught how to identify junk mail even if it's from a trusted source.

(I) Data Security, protection, and backup

Data security refers to the protection of data's confidentiality, availability, and integrity. "Data protection" refers to the protection of personal data against misuse by third parties. "Data backup" refers to the copying of existing data to prevent its loss.

PUBLISHED BY
The Supreme Court of Ohio