

6A-14.012 Florida College System Institution Safety Requirements

(1) The purpose of this rule is to establish requirements relating to safety, security, threat management, emergency preparedness, reporting, training, and compliance monitoring for Florida College System institutions pursuant to Sections 30.15, 943.082, 1003.25, and 1006.601, F.S.

(2) Definitions.

(a) “Active assailant” means any individual actively engaged in killing, attempting to kill, or posing an immediate and ongoing threat to kill or seriously injure persons in a public postsecondary educational institution setting.

(b) “Campus” means any facility, site, center, branch, instructional location, or other real property owned, leased, operated, or controlled by a Florida College System institution.

(c) “Certified guardian” means an employee of a Florida College System institution, excluding students, who has been certified pursuant to Section 30.15(1)(k), F.S., and appointed by the institution president to serve in a guardian capacity under Section 1006.601(2), F.S.

(d) “Division” means the Division of Florida Colleges within the Florida Department of Education.

(e) “Education records” means records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution, as defined in the Family Educational Rights and Privacy Act (FERPA) and is implementing regulations, 20 U.S.C. s. 1232g, 34 C.F.R. Part 99.

(f) “Institution” means a Florida College System institution as defined in Section 1000.21(3), F.S.

(g) “Florida Harm Prevention and Threat Management Model” or “Florida Model” means the Florida-specific behavioral threat management process used in K-12 public schools pursuant to Rule 6A-1.0019, F.A.C.

(h) “Florida Postsecondary Threat Management Protocol” or “Florida Postsecondary Protocol” means the threat management process and required documentation for threat management outlined in this rule to comply with Section 1006.601, F.S., wherein threats and reports of concerning behaviors or concerning communications are categorized as having a low, medium, or high level of concern.

(i) “Institution Safety Contact” means each institution’s current employee who is the first person to report or to be contacted regarding campus safety threats or regarding compliance with this rule.

(j) “Public Safety Agency” has the same meaning as provided in Section 365.171(3)(d), F.S.

(k) “Threat management” means the multipart process by which institutions identify individuals exhibiting threatening or other concerning behavior, assess the risk of harm, and coordinate appropriate interventions and services for such individuals.

(l) “Triage” or “Triage team” means the person or team responsible for initial review of all reports of concerning behavior, concerning communication, or threats, no matter how initially received, and triaging those reports to the appropriate team within the institution that is best equipped to handle the issue.

(m) “Violence” means an act or attempted act of force, threat, intimidation, harassment, stalking, assault, battery, weapons offense, or other conduct that poses a threat to the safety or well-being of students, faculty, staff, or visitors.

(3) Response Plans. Each institution’s Board of Trustees must adopt the following response plans, which may be included as a clearly delineated portion of its emergency preparedness plan or as a stand-alone plan:

(a) An active assailant response plan, which establishes procedures for immediate response to an active assailant incident, that:

1. Requires all faculty, staff, and students to annually complete active assailant preparedness training appropriate for their role.

2. Identifies specifically by position title the personnel authorized to issue emergency alerts;

3. Provides procedures for evacuation, lockdown, shelter-in-place, incident command, communication, and post-incident recovery; and

4. Includes an emergency notification process, which at a minimum describes methods for issuing emergency notifications to the campus community on active threats and crimes considered to be a threat to students, faculty, and staff, as required by 20 U.S.C. § 1092(f)(3). The process must identify all personnel responsible for issuing such emergency notifications. Notifications must be provided in a

manner that is timely, that withholds the names of victims as confidential, and that will aid in the prevention of similar occurrences.

(b) In cooperation with local law enforcement agencies and local government, a family reunification plan to reunite students and employees with their families in the event that an institution is closed or unexpectedly evacuated due to a natural or manmade disaster.

(4) Florida Postsecondary Threat Management Protocol (Florida Postsecondary Protocol). Each institution must establish threat management teams and must adopt policies and procedures for threat assessment as follows:

(a) Threat Management. The president of each institution must establish a Threat Management Team (“TMT”) whose duties include the coordination of resources and assessment and intervention with students whose behavior may pose a threat to the safety of the institution, institution staff, or other students. Institutions with multiple campuses may establish more than one TMT. Each TMT must be comprised of four (4) members (“Core Four”), at a minimum, including an administrator, a sworn law enforcement officer, a student services or counseling team member, and a member with expertise in instruction, which may be a faculty member, dean, or department head. The president is responsible for appointing TMT members.

1. If none of the team members are familiar with the student of concern, the TMT must attempt to consult with someone who is familiar with the student, whether on or off campus, to provide background information to the TMT. Consulting individuals do not have to complete Florida Postsecondary Protocol training and must not participate in the decision-making process.

2. For the 2026-2027 school year, TMT members must be appointed no later than October 30, 2026. Thereafter, TMT members must be appointed prior to the start of the fall term each year.

3. The president must also designate an institution triager or triage team to receive, review and triage all reports of concerning behavior, concerning communication, or threats, no matter how initially received. The triager will document basic information about the reported concern or threat and will determine if the report has a factual basis and whether it should be referred to the TMT or to another

campus team, depending on the type of harm or risk. Those responsible for triage may be members of the TMT or may be separate, but must receive Florida Postsecondary Protocol training, as required by paragraph (4)(d).

4. An additional administrator, who is not part of the TMT, must be assigned to review and approve completed threat management documentation, including the final level of concern and disposition of the case. Administrators assigned to this reviewer role must receive Florida Postsecondary Protocol training, as required by paragraph (4)(d).

(b) Protocol. Each TMT must use the process outlined in the Florida Postsecondary Threat Management Protocol Manual, Form FPP-01, incorporated by reference (<http://flrules.org/Gateway/reference.asp?No=Ref-20036>), effective October 2026, to assess the behavior of students who may pose a threat of harm to others and to coordinate intervention and services for such students. All reported threats or concerning behaviors and communications, even those determined to be unfounded, must be documented, along with any resultant action, using the standardized Florida Postsecondary Threat Management Protocol Intake and Disposition Form, Form FPP-02, incorporated by reference (<http://flrules.org/Gateway/reference.asp?No=Ref-20037>), effective October 2026. Form FPP-02 may be digitized and integrated into existing records management software used by institutions, as long as the same information is captured in the same format and the information can be transmitted to receiving school districts or other postsecondary institutions where the student enrolls.

(c) Meetings. At a minimum, the Core Four members of each TMT must meet as often as needed for the TMT to fulfill its duties, but no less than monthly. Institutions must adopt policies requiring TMTs to maintain documentation of their meetings, including meeting dates, team members in attendance, cases discussed, and actions taken. If the TMT has no active cases to discuss, they must document any other items discussed at their meeting and may use the time to discuss matters referred to other teams for response, to review patterns and clusters of reported behaviors, or to engage in additional training and tabletop exercises.

(d) Training. All assigned members of the TMT and those responsible for triage and final administrative review must receive initial training in the Florida Postsecondary Protocol, including information from the Florida Model that is appropriate for postsecondary review of records received from K-12 schools. For the 2026-27 school year, training must be completed no later than December 18, 2026, with annual initial or refresher training, as appropriate, required thereafter prior to the start of fall term.

(e) Dual Enrollment. If the student of concern is a dual enrollment student from a Florida public school, and the threatening or concerning behavior occurs on a college site or in a college class, the college TMT must conduct the threat assessment and manage the student, in continued consultation with the K-12 school's threat management team. If the college determines that the student may no longer participate in dual enrollment, the student's K-12 school will determine next steps for student support. If the incident does not occur on a college campus or in a college class, and the college is notified first of the incident, the college must refer the matter to the student's K-12 school for the school to conduct the threat assessment and manage the student using the Florida Model with consultation from the college's TMT.

(5) Student Mental Health and Behavioral Health Supports. Each institution must adopt policies and procedures to support student mental health and behavioral health intervention, including:

(a) Required training for faculty to learn how to detect and respond to students exhibiting behavioral health concerns, including institution-specific direction for faculty on where to refer students with mental or behavioral health concerns;

(b) Procedures to connect students to institutional and community-based behavioral health services, including crisis intervention; and

(c) Posting and maintaining on its website and in conspicuous locations on each campus a mental health awareness and suicide prevention notice as specified in Section 1006.601(4), F.S.

(6) Student, Faculty, and Staff Victim Supports. Each institution must adopt policies and procedures to support students, faculty, and staff who are victims of violence, attempted violence, or credible threats as defined in Section 784.048(1)(c), F.S.

(a) Such policies must include available support measures and procedures for timely communication and status updates to the affected person or persons regarding institution actions.

(b) Such policies may include, and are not limited to, options for work or class relocation, security escorts, and restrictions on access to campus locations by individuals who pose a threat.

(7) Florida Postsecondary Security Risk Assessment.

(a) Each institution, in collaboration with appropriate public safety agencies, must annually conduct a security risk assessment for each site using the Florida Postsecondary Security Risk Assessment.

Documented findings must be used by each institution to identify risks, vulnerabilities, and corrective actions; prioritize security improvements; and inform institutional safety planning and funding requests.

(b) In accordance with Section 119.071(3)(a), F.S., data and information related to the Florida Postsecondary Security Risk Assessment is confidential and exempt from public records requirements.

(c) Beginning in the 2026-27 academic year, the security risk assessment must be submitted to the Division no later than December 18, 2026. Beginning in the 2027-28 academic year, the security risk assessment must be submitted to the Division no later than October 1 each year.

(8) Mobile Suspicious Activity Reporting Tool. Each institution must implement a mobile suspicious activity reporting tool that allows students and the community to relay information anonymously concerning unsafe, potentially harmful, dangerous, violent, or criminal activities, or the threat of these activities, to appropriate public safety agencies and school officials. Institutions may use FortifyFL for this purpose pursuant to Section 943.082, F.S. Institutions must promote the use of their adopted mobile suspicious activity reporting tool(s) by:

(a) Advertising the tool on the institution website;

(b) Installing the tool on institution-issued mobile devices; and

(c) Bookmarking or otherwise prominently linking the tool on institution-maintained computer devices.

(9) Guardian Program. A Florida College System institution may participate in the Chris Hixon, Coach Aaron Feis, and Coach Scott Beigel Guardian Program (“Guardian Program”) pursuant to Sections 30.15(1)(k) and 1006.601(2), F.S. An institution that elects to participate in the Guardian Program must:

(a) Adopt institutional policies governing appointment, supervision, and deployment of certified school guardians;

(b) Ensure each guardian is certified in accordance with Section 30.15(1)(k), F.S.;

(c) Ensure each guardian is appointed by the institution president;

(d) Maintain documentation of appointment, certification, annual qualification, and separation;

(e) Report required guardian data in the manner and timeline prescribed by the Florida Department of Law Enforcement; and

(f) If contracting with a law enforcement agency for guardian training, provide required notice to the sheriff in the institution’s county prior to execution of the contract.

(10) Threat Management Records.

(a) Threat management records include all corresponding documentation related to the reporting, evaluation, intervention, and management of threat assessment evaluations and intervention services. Threat management records include psychological evaluations, therapeutic treatment plans, and therapy or progress notes, if those records are documented as evidence in or otherwise made a part of a threat assessment. All reports of concerning behavior, concerning communication, or threats must be transferred, regardless of the outcome or level of concern. Threat management records are considered education records, as defined by FERPA. Each institution must adopt procedures for the secure receipt, handling, access, retention, and disclosure of threat management records that are consistent with FERPA and that include the following:

(b) Receipt and review of threat management records from K-12 schools. Procedures must include:

1. A process by which threat management records are requested from the school district where a student last attended or is currently attending if dual enrolled. Requests for threat management records

must be made after enrollment. Upon availability, such requests to a district must be made through the Florida Safety and Threat Management Portal;

2. A process for review of K-12 threat management records that includes prioritization of student records based on the level of concern and recency of their threat assessment; and

3. A process for review of psychological evaluations, therapeutic treatment plans, and therapy or progress notes received from K-12 schools. Review of these records must be handled by appropriate institution staff with a legitimate educational interest in the records. These records must not be shared with the institution's disability services office, unless authorized by the student.

(c) Retention of K-12 records. Institutions are not responsible for maintaining copies of K-12 threat management records, as they will continue to be maintained in the Florida Safety and Threat Management Portal pursuant to Rules 6A-1.0019 and 6A-1.0955, F.A.C. If an institution attaches or otherwise incorporates copies of K-12 threat management records into a threat assessment being completed at the college level, the postsecondary threat management records must be maintained in accordance with paragraph (10)(f).

(d) Receipt and review of postsecondary threat management records. Procedures must include:

1. A process by which threat management records are requested from other FCS institutions and state universities upon enrollment at an FCS institution; and

2. A process for review of postsecondary threat management records, that includes prioritization of student records based on the level of concern and recency of their threat assessment.

(e) Transfer of postsecondary records. Procedures must include a process for securely transferring threat management records within five (5) business days to school districts, FCS institutions, and state universities, upon request. Postsecondary psychological evaluations, therapeutic treatment plans, and therapy or progress notes are only transferred when they are documented as evidence in or otherwise made a part of a threat assessment.

(f) Retention of postsecondary records. Postsecondary threat management records must be maintained for minimum of ten (10) years.

(11) Reporting Requirements.

(a) By October 1 of each year, each institution must submit reports and certifications in the manner and format prescribed by the Division, including:

1. Annual certification that all employees and students have completed active assailant preparedness training;

2. Annual certification that the institution has reviewed and its Board of Trustees has approved the institution's active assailant response plan;

3. Annual certification that the institution has reviewed and its Board of Trustees has approved the institution's family reunification plan;

4. Annual certification that the institution's threat management process has been reviewed, the members have been designated and trained, and individuals eligible to review student threat assessment records have been designated and trained; and

5. The annual Florida Postsecondary Security Risk Assessment pursuant to subsection (7) of this rule.

(b) By August 15 each year, each institution must report the name, phone number, and email address for their Institution Safety Contact to the Division to FCSSafety@fldoe.org. If the Institution Safety Contact changes during the year, the institution must notify the Division within two business days.

(c) For the 2026-2027 academic year, the reporting required under paragraphs (a) and (b) must be submitted by December 18, 2026.

(12) Corrective Action and Enforcement.

(a) Institutions must maintain sufficient records demonstrating that requirements of this rule have been met and must provide such records to the Division upon request.

(b) If the Division determines an institution is not in compliance with applicable law or this rule, the Division shall notify the institution and may require corrective action.

(c) Compliance with safety requirements set forth in Florida Statutes and this rule is subject to enforcement by the Commissioner of Education and the State Board of Education using mechanisms provided in Section 1008.32, F.S.

Rulemaking Authority 1001.02(1), (2)(n), 1003.25(4), 1006.601(4)(b)3., (5) FS. Law Implemented 30.15.

943.082, 1003.25, 1006.601 FS. History- New