PANIC BUTTON SYSTEMS ON CAMPUS

Best Practices, Compliance Requirements & Implementation Guidance

Written by Lance Klukas, DMI Security Consultant

EXECUTIVE SUMMARY

- Panic button systems represent one of the most direct investments a campus can make in rapid-response emergency preparedness.
- Wisconsin technical colleges operate under a unique risk profile — serving diverse adult learners, evening programs, satellite campuses, and high-traffic trade labs — making reliable, campus-wide alert systems especially critical.
- This article reviews proven deployment strategies, applicable federal and Wisconsin-specific regulations, and an honest assessment of the technology's strengths and limitations to help security and risk management professionals make informed decisions.

Panic button systems provide a mechanism for students, faculty, and staff to instantly summon emergency assistance without having to dial a phone, speaking aloud, or navigate certain systems under stress. When properly integrated with campus systems and local law enforcement, they can reduce emergency response times.

TYPES OF PANIC BUTTON SYSTEMS

- **Fixed/Hardwired Panic Buttons**: Physical buttons mounted typically on desks, welcome areas, counseling offices, financial aid/cashier, and faculty offices in high-risk programs. When activated, they transmit a silent alarm directly to campus security and/or 911. These are among the most reliable and tamper-resistant options available.
- **Wireless or Portable Panic Fobs**: Small, wearable devices worn by staff. When activated within range of a receiver, these transmit an alarm and often GPS coordinates. Ideal for counselors, financial aid staff, student services personnel, and evening staff.
- **Mobile App Panic Buttons**: Smartphone apps (e.g., LiveSafe, Rave Guardian, CampusSafe) that allow users to trigger an alert from their personal device. These apps typically share GPS location data, may open a silent audio channel, and can notify both campus security and 911 simultaneously. Especially effective for coverage across dispersed or satellite campuses.
- **Computer Software / Desktop Panic Buttons**: Software installed on campus workstations that enables a single keypress to trigger an emergency alert. This is particularly valuable for administrative staff, lab instructors, and student success center personnel who may face a potential threat while at their desk. Many solutions integrate with existing systems.
- **Blue Light / Emergency Call Stations:** Outdoor (or indoor) mounted emergency call stations, typically with visible blue lights. When activated, they connect directly to campus security or 911 and illuminate assisting responders in locating the caller.

LEGISLATION, REGULATIONS & COMPLIANCE REQUIREMENTS

The **Clery Act** (20 U.S.C. § 1092(f)) is the primary federal statute governing campus safety. Key Clery Act obligations relevant to panic buttons and emergency notification:

- Emergency Notification: Institutions must have procedures for immediately notifying the campus community upon confirmation of a significant emergency or dangerous situation. Panic buttons are often integrated into this notification infrastructure.
- Emergency Response and Evacuation Procedures: Colleges must annually publicize emergency response, evacuation, and testing procedures. Panic button systems should be explicitly referenced in these disclosures.
- Annual Security Report (ASR): Campus safety policies, including alert systems, must be documented and published. The existence and coverage of panic button infrastructure should be included.
- Timely Warning Policy: When a Clery crime occurs that poses an ongoing threat, timely warnings must be issued. Panic button activations that result in Clery crimes may trigger this obligation.

Americans with Disabilities Act (ADA) — Title II

Under ADA Title II, public entities must ensure that emergency communications are accessible to individuals with disabilities. Panic button systems must be operable by persons with mobility, visual, or cognitive impairments. Considerations include:

- Button placement at accessible heights (ADA standards require operable components between 15" and 48" AFF)
- Non-verbal alert options for individuals with speech impairments
- Mobile app interfaces designed for screen reader compatibility
- Visual and tactile indicators for systems in areas used by individuals with hearing impairments

OSHA General Duty Clause (Section 5(a)(1) — 29 U.S.C. § 654)

The OSHA General Duty Clause requires employers to provide a workplace free from recognized hazards likely to cause death or serious harm. For our colleges, this creates an implicit obligation to provide panic or duress alert mechanisms in environments where employees face elevated risks, such as:

- Financial aid offices
- Counseling and mental health services
- Human resources
- Evening and lone-worker situations
- Healthcare simulation labs and clinical training environments

OSHA's Workplace Violence Prevention guidelines (OSHA 3148) specifically recommend the use of duress alarms in settings where violence risk is elevated, including healthcare and social service environments.

Wisconsin Statute § 36.11 / WTCS System Requirements

Under Wisconsin Statute § 36.11, each college is responsible for maintaining campus safety programs that meet or exceed state and federal standards and requires all colleges to maintain Emergency Operations Plans (EOPs) that address communication and notification infrastructure, including alarm systems.

Title IX — Campus Safety & Retaliation Protections
While Title IX (20 U.S.C. § 1681) primarily governs sex discrimination, its implementing regulations require institutions to maintain confidential reporting mechanisms and protect complainants from retaliation. Panic buttons used in Title IX-related contexts (e.g., accessible from a Title IX coordinator's office, or as a resource for individuals reporting harassment) must be maintained in a manner consistent with confidentiality obligations. Activations and records of use must be managed carefully to protect reporter identity.

PROS AND CONS:

✓ ADVANTAGES / PROS	✗ LIMITATIONS / CONS
Rapid, one-touch activation; no need to speak or navigate menus under stress	False activations waste emergency resources and can desensitize responders
Immediate location data transmitted to dispatch, reducing response time	Fixed systems create coverage gaps in areas not pre-wired
Silent activation protects the user from escalating a confrontation	Mobile apps require smartphone ownership and cellular/Wi-Fi coverage
Builds demonstrable Clery Act and OSHA compliance documentation	GPS accuracy can be poor indoors; location data may be imprecise
Reduces liability exposure by showing proactive duty-of-care investment	Initial installation and integration costs can be significant ($500–$3,000+ per node)
Supports lone worker safety for after-hours and satellite campus staff	Systems require regular testing, maintenance, and battery checks
Mobile apps extend coverage to parking lots, satellite sites, and transit areas	Staff must be trained; untrained users may not activate or may activate incorrectly
Visible systems (blue light towers) act as crime deterrents	Privacy concerns around continuous location tracking (for wearable fobs)
Can integrate with access control, cameras, and mass notification systems	Cybersecurity vulnerabilities in IP-based and app-based systems
Relatively low ongoing cost once infrastructure is established	Vendor dependency: proprietary systems can create long-term lock-in

✓ ADVANTAGES / PROS	✗ LIMITATIONS / CONS
Provides psychological safety benefits; staff feel supported and protected	Wireless systems may be subject to radio frequency interference
Can be activated discreetly during mental health or domestic violence incidents	Response is only as effective as the campus security capacity behind it

BEST PRACTICES

Conduct a Formal Site Risk Assessment First

Before deploying any system, identify high-risk zones: financial offices, counseling, parking structures, and isolated corridors. The assessment should inform placement priorities and technology selection.

Integrate with Dispatch and Law Enforcement

Panic button activations should route directly to a monitored dispatch service. For colleges that contract law enforcement services or share dispatch with a municipal agency, formal integration agreements shall be in place. The system needs to be tested regularly with the actual receiving agency to ensure signal delivery, location accuracy, and response protocol clarity.

Establish a False Alarm Response Protocol

False activations are inevitable. Establish a clear protocol for how staff responds to activations, assume real until confirmed otherwise, and track false alarm rates. High false alarm rates should trigger retraining, not reduced response. Chronic false alarms from specific devices should prompt investigation and remediation.

Train All Personnel

Training must reach all personnel, not just full-time employees. Training should include: how to activate each device type available on their campus, what happens after activation, and how to communicate location information if verbal communication is possible.

Test Routinely and Document Everything

Conduct full system tests no less than quarterly, with at least one unannounced test annually. Document all test results, response times, and any system failures. This documentation is essential for Clery Act compliance and provides critical evidence of due diligence in the event of litigation.

Address ADA Accessibility at Every Installation

Before finalizing any installation, verify ADA compliance for operable height, approach clearance, and alternative signaling. Engage your institution's ADA/Section 504 coordinator in the review process. Document accessibility assessments for each installation location.

Protect System Cybersecurity

For IP-based, cloud-connected, and mobile app systems, conduct a cybersecurity review as part of procurement. Ensure the vendor follows current NIST Cybersecurity Framework guidelines, that data is encrypted in transit and at rest, and that your IT security team has visibility into system access logs. A panic button system that can be spoofed, disabled remotely, or flooded with false alerts is a security liability, not an asset.

VENDOR SELECTION CONSIDERATIONS

When evaluating panic button vendors, assess the following criteria:

KEY VENDOR EVALUATION CRITERIA

- Integration capability: Does the system integrate with your existing systems, access control, and mass notification platforms?
- Monitoring reliability: Is the backend monitored 24/7? What is the SLA for signal delivery and response acknowledgment?
- Scalability: Can the system expand across satellite campuses without significant re-infrastructure investment?
- Training and onboarding: Does the vendor provide comprehensive staff training and refresher resources?
- Compliance documentation: Does the vendor provide documentation suitable for Clery Act annual reporting?
- Data retention and privacy policies: How long is activation data retained? Who has access? Is data shared with third parties?
- Contract terms: Avoid long-term proprietary lock-in without performance guarantees and exit provisions.
- References: Request references from comparable higher education institutions, preferably in the Midwest or Wisconsin.

RECOMMENDATIONS

- Audit existing panic button coverage and document gaps using a campus map overlay
- Verify all existing systems are operational and tested against dispatch
- Review Annual Security Report disclosures for accuracy and completeness regarding alert systems
- Conduct at least four system tests per year with full dispatch notification; document all results
- Review and refresh all training materials; re-train all new and returning personnel

CONCLUSION

Panic button systems can reduce response times, demonstrate regulatory compliance, and communicate a culture of care and preparedness to the students and employees who rely on these institutions every day. However, technology alone does not create safety. The most sophisticated panic button system is only as effective as the setup behind it, the training that

supports it, and the institutional commitment to test, maintain, and improve it over time. Risk management professionals are encouraged to approach panic button deployment not as a one-time capital project, but as an ongoing operational commitment integrated into campus safety.

OTHER RESOURCES:

- DMI KB (Slab) Article: https://dmikb.slab.com/posts/panic-buttons-06srdz5x
- 7 Questions to Ask When Evaluating Panic Button Solutions (Campus Safety Article)
- Panic Buttons Aren't Just for Active Shooters (Campus Safety Article)
- Intrado OneAlert™ for Education