PacStates
Integrated Business Technology
One Company, One Call

Just as protecting your home is vital during a threat, any threat to security is always a serious concern. The increasing crime, shutdowns, trespassing issues of all kinds, as well as rioting and looting situations, brought heightened awareness of the importance of keeping your commercial building safe and secure.

How do you improve building safety and security to protect yourself, your business, your employees, and your clients? Perhaps the most important thing to remember, first and foremost " Is that securing **your property must be proactive rather than reactive.**

Do not wait for something to happen before taking the necessary steps.

To maximize safety and security, we've put together our top 10 Tips For a safety and security review before we meet to discuss your strategic safety plan.

10 TIPS FOR BUILDING SECURITY

1. Know the risks you are facing. Our experts will teach you how to protect yourself even if you do not know where the threats are coming from at the beginning.
Once you have identified the risks, you can develop a comprehensive plan that best suits your needs. PacStates is commercial access control and facility security specialists and are always in service to our community.

2. Secure Perimeter Your first line of defense is risk analysis, and you must identify the blind spots in and around your building.
Safety and security are greatly enhanced by installing adequate lighting in parking lots, break areas, stairwells, and dark hallways. Consider external motion-activated and internal lights that make your building look occupied even when no one is around.
If there is landscaping around the building, keep it groomed and shrubs/trees trimmed to eliminate areas where someone can hide and prevent window or roof invasion.

3. Access Control and Regulation We recommend combining two techniques â€“ natural access control and technology using an electronic access control system.
Natural access control uses the building and landscaping features to guide people entering and exiting. Limiting access to your building or facility to one or two entrances that are fully monitored discourages intruders while closing off potential escape routes.

Further monitoring and controlling access to your building is through an electronic access control system which enables you to control who accesses your structure, when they can access it, and where they can go once inside.
Moreover, assigning different levels of access to other individuals is possible. For instance, visitors may be granted access only to public areas; contractors are allowed access for a limited period of time and are restricted to certain areas only. There are also options for control for certain employees who may be allowed access to some high-security regions like IT rooms, etc. Access control systems create audit trails and reports that can be generated should a security breach occur.
PacStates is your One company, one call resource, and go-to resource for all of your safety, cameras, communications, and technology needs. Reach out to us for a free onsite review.

4. Security Cameras For buildings requiring enhanced security, a closed-circuit TV system is an effective tool for monitoring your building.
It's vital to install cameras so maximum coverage is achieved strategically.

A great example would be to consider installing one unit in an "airlock" door system entry. This would allow you to capture extended footage of who gained access to or exits the premises.
More than being tools for recording all activity in your building, they also serve as deterrents and contribute to creating a safe environment for your facility. PacStates consults, recommends, and installs a wide range of security cameras for commercial properties to fit every situation. Reach out to us for a free onsite review.

5. Key Access If an electronic access control system is not applicable for your building, having an established procedure for controlling and distributing keys is important. Assign key custodianship and the responsibility of locking and unlocking the office/building to a few select individuals.
For full accountability, physical keys should be numbered and assigned only to specific people. And a periodic audit of the actual keys is a must.
The procedure should include precise instructions on opening and locking the office, including checking washrooms, closets, or areas where someone might hide.

6. Dedicated entry system As an extra layer of defense against unauthorized access, having a person or persons dedicated to greeting and check-in visitors is a good idea. This allows you to closely inspect credentials and IDs and ensures security information goes through only a single point.
If a receptionist isn't available, you may opt for a dedicated phone in your building or office lobby and calls would route to a designated receiver. Visitors are tracked through a sign-in station.

7. Anti Theft Devices, Secure Doors, and Airlock Rooms These are minor investments that remarkably enhance security.

8. Cyber Security Protecting against cyber attacks is equally as important as keeping your building secure. Investing in the most up to date protection from viruses, Trojans, worms,

malware, and spyware should also be a security priority. Your cyber security plan should include use agreements and education as well as the usual firewalls, security for wireless internet routers, as well as secure backups for data in case of a cyber attack.

9. Security Policy There are many policies that your company can adapt depending on your particular requirements. What are examples?

- "Clean Desk Policy" or the practice of having all essential documents and valuable equipment removed from the desk and secured before ending the work day reduces the potential for theft.
- "Chain of possession ." Deliveries should be handed directly to the recipient and not just left unattended on the desk or outside his office.
- To prevent names from being used by criminals to justify their presence in a restricted area, job titles should not be posted on any directory that is publicly accessible.
- Employees should be required to wear their uniforms or attire with logos as well as ID badges/access cards at all times while on-premises.

10. Employee Training A significant percentage of breaches result from insider action â€ “ employees. Training employees on best practices and policies like the ones written above to avoid security risks and breaches due to human error should be a top priority.
Finally, constant communication on potential security issues helps keep security and safety awareness high.