PacStates
Integrated Business Technology
One Company, One Call

Building Security
CHECKLIST FOR BUILDING SECURITY

Keeping your business safe and secure should always be a serious concern. The recent looting and acts of violence around the protests remind us that we need to be more aware and our surroundings and current events even if you are not interested in following political issues.

Just as there are advancements in security and safety technology, criminals have become equally advanced and increasingly creative.

PacStates offers an entirely FREE comprehensive evaluation with one of our experts to help improve your building security, protect yourself, your business, your employees, and your clients.

The most important step anyone can do is to prioritize your safety and security appropriately. Be proactive rather than reactive. Do not wait for things to happen before taking the necessary protective steps.

We use these guidelines to help you maximize safety and security measures:

1. Assess and identify risks. Ask an expert! Whether it is Cybersecurity issues or building safety measures, ask an expert, create an opportunity for employees to share openly about needed safety measures, and never assume!

Once you have identified the risks involved, draw up a comprehensive plan covering all of your concerns, and prioritize them.

2. A secure perimeter is your first line of defense. Our commercial access control and facility security specialist will review and add hidden areas of concern you may need to be aware of.

3. Consider Access Control. Find ways to safely make entry to your building by using modern thermal imaging solutions, cameras, and even disinfecting methods. You will also want to discourage intruders while closing off potential escape routes. This can be done by combining two techniques:

   1. Natural access control (using the building itself or landscaping features to guide people as they enter and exit).
   2. Technology- using electronic access control systems, enabling you to control who accesses your structure by determining if they are safe to enter, when they can access, and where they can go when they enter.

4. Have a recognizable reception area, or at minimum, a receptionist adds an extra layer of defense against unauthorized access and gives you the ability to conduct a closer inspection of temperatures, credentials, and ID at a single point of entry. Because this will tie up your receptionist, we highly recommend you re-visit your CALL FLOW options on your phone system to ensure no your incoming call volume doesn't suffer.

7. Thermography sensing cameras, decontamination units, anti-theft devices, secure doors, and airlock rooms are generally minor investments that can also enhance building safety.

8. Cybersecurity. Investing in a superior protection plan from viruses, Trojans, worms, malware, and spyware should be a top security priority. Your cybersecurity plan should include firewalls, security for wireless Internet routers, as well as secure backups for data in case of a malware or cyber attack.

9. Employee Training. A significant percentage of breaches result from insider action – employees who either accidentally or deliberately have the same effect on the business, so training, checks, balances, and monitoring are critical. Training employees on best practices and policies in a way that promotes buy-in and accountability are very helpful.

Employees should also be made aware of:

- Create and vigilantly maintain a "Clean Desk" policy. This is the practice of having all valuables, essential documents, equipment, etc. stored away from the desk and secured before walking away from their desk or ending the workday.
- "Chain of possession." Deliveries should be handed directly to their intended recipient and never just left unattended.
- Do not list job titles in any publicly accessible area to prevent names from being used to leverage access to a restricted location.
- Require team members and visitors to wear their ID badges/access cards at all times while on-premises.

Finally, encourage positive and constant communication on any potential security issues or threats. This will help keep security and safety awareness high.