AVIGILON™

OFFICE SECURITY AUDIT & SAFETY CHECKLIST

Assess and improve your current physical security

MOTOROLA SOLUTIONS

OFFICE SECURITY AUDIT & SAFETY CHECKLIST

Security is a priority when you run a facility, whether big or small, and can include measures such as locks and security cameras, as well as protocols for managing access to the building and monitoring activity within it. To measure the effectiveness of your physical security, an assessment will evaluate how well your building and its occupants are protected from potential threats.

One way to determine the effectiveness of your facility's safety measures is by conducting a physical security audit, which helps identify potential weaknesses and threats, ensuring that the facility is adequately protected against threats such as burglaries, data breaches, and unauthorized access. According to research by Ponemon Institute LLC, organizations that test their security measures have much higher confidence in their overall physical security, which allows them to concentrate on more important business aspects.

It's recommended to hire a third-party physical security auditor to ensure that you meet regulatory safety requirements, industry standards and are taking into account the latest known vulnerabilities. However, not every organization has the budget to do so. If you're not yet ready to hire an auditor, putting together an internal physical security checklist can help strengthen your security measures.

In this guide, we will provide you with an office security checklist that you can use to assess your current physical security and identify what areas need improvement. While this office safety checklist is a helpful guide, it doesn't replace a professional audit and certification. We recommend speaking to a physical security auditor after running your own building safety checklist to ensure nothing is overlooked.

WHAT IS A PHYSICAL SECURITY ASSESSMENT?

Also called a security audit, a physical security assessment is a systematic evaluation of a facility and its security measures, with the goal of identifying potential vulnerabilities and areas for improvement.

This can involve a review of security policies and procedures, an inspection of the physical premises, load-testing any security systems and interviews with employees. The physical security risk assessment should focus on the protection of people, assets and information, and should consider potential threats such as burglaries, natural disasters and internal theft.

The purpose of an office security audit is to ensure that a facility is adequately protected against potential threats and that security measures are effective and appropriate. A good office security audit will also ensure all security equipment in place is properly running in case of a breach or emergency.

What happens during a physical risk assessment?

There are several key steps to a physical security auditing checklist:

- **Policy and procedure overview:** This step includes reviewing any access control measures, security patrols, and incident response protocols to determine any weaknesses or inconsistencies in security practices. A physical security auditor can provide recommendations for improvement, if needed.
- **Inspection of the physical premises:** In this part of a physical security risk assessment, an auditor will inspect building construction, layout, lighting and landscaping for deficiencies in the infrastructure that can be easily exploited and provide recommendations for upgrades or enhancements.
- **Testing your security systems:** Technology should function at full capacity, and it's important to evaluate any electronic locks, security cameras and alarm systems to ensure they are all in working order.
- **Employee interviews:** The final step in an office security assessment will help you gain a better understanding of how susceptible your employees are to malicious actors trying to take advantage of them to gain access to your facility, as well as help ensure that they are aware of the proper protocols when a breach or natural disaster occurs.

Overall, a physical security assessment checklist is an important tool for ensuring the safety and security of a facility. By regularly conducting risk assessments and implementing security recommendations, facilities can reduce the risk of breaches and maintain a safe and secure working environment.

How often do I need to conduct a physical security risk assessment?

By regularly conducting assessments, facilities can identify any gaps in their security measures and take steps to address and improve them. This can help reduce the risk of security breaches and maintain a safe and secure environment for employees and assets.

Generally, it is recommended to perform a thorough building security checklist every year. However, depending on the location, size and industry of the organization, the frequency may vary. Larger organizations with hundreds of employees may want to run more frequent audits.

PHYSICAL SECURITY AUDIT CHECKLIST FOR OFFICES AND COMMERCIAL BUILDINGS

While a comprehensive physical security risk assessment should be carried out by a professional, there's still some value in conducting your own as part of a proactive security strategy. Follow the process below to evaluate how ready your facility is when a breach occurs:

Office policies and procedures security checklist

To conduct an office security checklist, start with the measures and protocols that are in place to protect people, assets, and information from potential threats.

If you don't have a written policy, now is a great time to outline all your security measures. If your office has a procedure code, it is important to regularly review and update policies regularly. As part of a physical security assessment, this is necessary to ensure they are effective.

The goal of reviewing policies for your office security checklist is to identify any gaps or inconsistencies in security practices and provide recommendations for improvement. To evaluate if your current policies and procedures are working, ask the following questions:

- What is the scope of your security review? This could be the entire organization, a specific department or business unit, or a particular process or system.
- Do you have existing internal security policies or procedures?
- Are there any relevant regulatory standards or industry procedures your organization should follow?
- Is each policy still relevant and up to date? Consider any changes in the organization, technology, or threats that may have occurred since the policy was last reviewed.
- Are there any gaps or inconsistencies in your current policies? For example, do different policies conflict with each other, or do some policies provide enough guidance on how to handle certain situations?
- Are there any controls or requirements missing from your office security checklist that need to be reviewed or tested to ensure compliance?
- Do you have a way to document the results of regular office building security audits, including any recommendations for improving security?

Inspection checklist for physical premises

After you've reviewed and evaluated your current policies and procedures, the next thing on your physical security risk assessment checklist is to inspect your actual facility. This includes checking your physical structures and overall premises to identify anything that can affect the integrity of your physical security.

Maintenance is a commonly overlooked part of an office building security checklist, but having a clean, clutter-free space can make a big difference when it comes to security. A premise with debris, garbage or unkempt landscaping may be more of a target for criminals, while unorganized interiors can lead to slower responses during critical moments.

Use this checklist to check and inspect your facility's physical premises:

The exterior of the building

Are entry points, such as doors and windows, secure and in good working order? Are there any vulnerabilities, such as unsecured windows or doors, that could be exploited by potential intruders?

- ☐ Is all exterior lighting effective and in good working order?
- ☐ Do you have visible signage of private property with short walls or fences, if needed?
- ☐ Is the perimeter of the building secured and well-maintained?
- ☐ Are lawns landscaped, removing any weeds, leaves and debris?
- ☐ Are building exteriors clean and maintained, including regular exterior painting?

The interior of the building

- ☐ Are dark corners or unsecured areas given proper visibility and security measures?
- ☐ Does the facility layout give security personnel clear lines of sight to key entry points?
- ☐ Are all potential vulnerabilities, such as unsecured areas or weak points in the building's structure that could be exploited by potential intruders, addressed?
- ☐ Are your IT closets and storage areas well-organized?
- ☐ Do you have a way of maintaining visitor logs or records?
- ☐ Are pieces of interior furniture and any display items positioned properly so that all entrances and exits are clearly visible?
- ☐ Is there interior lighting that can remain on at night and when the office is empty to deter intruders?

Checklist for testing security systems

Most buildings today have security technology installed, such as video surveillance cameras, access control, alarms and building management systems. However, regular maintenance should be conducted to ensure they are still in good working order.

It's vital to regularly test your security technology during a building security risk assessment. This can include running reports to ensure no vulnerabilities have been missed, but should also involve load-testing your systems with simulated break-ins or security drills.

Here are a few key questions for your office security checklist:

Access control

- How are permissions granted and managed?
- How are access cards or tokens issued and managed?
- How are access logs and reports generated, and how often are they reviewed?
- How is the access control system integrated with other security controls (e.g. intrusion detection, firewalls and data encryption)?
- Are there any vulnerabilities or weaknesses in the access control system that could compromise security?
- Are there any incidents or breaches of access control security that have occurred in the past, and have you addressed those vulnerabilities?
- How reliable are your readers and locks?

Video security

- Are your security cameras all online and working properly?
- Do all cameras give a clear, high-definition image, even in varying lighting conditions?
- Are any high-risk areas fitted with security cameras?
- How is camera footage monitored? If you do not have 24/7 monitoring, do you have alerts set up for any suspicious activity?
- Is your video data storage secured?
- Do you have enough video data storage to meet industry standards for auditing?

Interviewing employees for office risk assessments

Interviewing employees should be a part of your physical security audit checklist. Talking to staff can provide valuable insights into how well security knowledge and practices are being communicated in your organization. With this, you can determine whether employees are aware of and trained on security protocols and whether they follow them in their daily work.

In addition, interviewing employees during a building safety checklist audit can help identify potential vulnerabilities in the security of a facility. Unfortunately, not everything can be detected during a physical security risk assessment of your premises and systems. For instance, your employees may have some security concerns that can turn into something serious if not addressed properly.

Interviewing employees can also help ensure they are aware of and prepared for potential risks and threats to the facility. By engaging with employees and providing them with information on security measures and protocols, you can help them feel more confident and prepared in the event of a security incident. This can help foster a culture of security at your facility and improve the overall safety of the workplace.

Here are some sample questions for a physical security audit checklist:

- Are employees aware of your company's security policy?
- What are the procedures for reporting security incidents or breaches?
- How can employees identify and avoid phishing attacks and other types of social engineering?
- What are the measures in place to protect the company's data and systems?
- What are the rules for accessing sensitive data and systems?
- Are employees aware of the potential risks and threats to the facility, and do they know how to respond in an emergency?

Building safety checklist for natural disasters

Natural disasters in the United States caused more than $280 billion in overall losses in 2021 alone. This number includes both private and commercial facilities.

While natural disasters can't be prevented, there are protocols and measures that can be set in place to mitigate damages. Below is a physical security checklist you can use to lessen the effects of natural disasters:

- ☐ Identify potential natural disasters prone to your area that could affect the facility, such as earthquakes, hurricanes or flooding.
- ☐ Develop a plan for responding to each type of disaster, including emergency evacuation procedures, emergency communications protocols and emergency supplies.
- ☐ Communicate the plan to all employees and conduct regular training and drills to ensure that everyone knows what to do in the event of a disaster.
- ☐ Install protective measures, such as reinforced walls, shutters or flood barriers, to reduce the risk of damage from natural disasters.
- ☐ Develop backup systems and emergency power sources to ensure that critical systems and equipment can continue to function in the event of a disaster.
- ☐ Create emergency supply kits and stockpiles to ensure that essential supplies, such as water, food and medical supplies, are available in the event of a disaster.
- ☐ Monitor weather conditions and warnings, and stay informed about potential natural disasters.
- ☐ Use weather monitoring and warning systems, such as sirens or alerts, to quickly and effectively communicate potential threats to employees and other occupants of the facility.

Is your organization prepared for security threats?

An office security checklist is vital in identifying potential vulnerabilities and threats. As a physical security risk assessment tool, a good security audit checklist can help facilities mitigate potential threats and maintain a safe and secure environment for employees and assets.

With the office building security checklists and guidelines outlined in this guide, businesses can conduct effective preliminary physical security audits and gain crucial insights into what to look for when working with professional building security auditors. This can provide peace of mind and ensure that a facility is adequately protected against potential threats, even as the security landscape continues to evolve.

MOTOROLA SOLUTIONS

AVIGILON™

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**