### Newsletter



INTERNATIONAL





## INSIDE THIS ISSUE

Travel Security is all about preparedness and avoiding danger. It's vital that individual travellers and travel managers receive realtime information about global incidents that may affect them. On the rare occasion that something dangerous does occur, Travel Security prepares you to cope with it.





At The Portfolio International, we understand that security is paramount in today's ever-evolving landscape of risks and challenges. For over a decade, we have been the trusted partner for individuals and organizations seeking unwavering protection and peace of mind. Our comprehensive suite of security services is tailored to safeguard what matters most – your people, assets, and operations.



# 8 best practices to protect your employees and office property

I. Visitor management system
Your front desk is your front line of defense. So
implement a <u>visitor management system</u> that
helps your front desk that does security the
welcoming way. Your visitor management system
will screen visitors, cross-reference them against a
blocklist, and send alerts to the necessary point of
contact if anything looks suspicious—all
automatically and discreetly in the background.
Plus, it will keep a record of the comings and
goings of each guest so that you'll know who's
onsite, when, and how often.

#### 2. Access control

Access control is a physical security method that controls or limits access to a space. In other words, it's a way to make sure everyone who walks through the door is meant to be there. Access control can look like an application on your phone, facial recognition, or a code to punch in. Having access control set up is a sure fire way to make sure you deter any unsavory characters from entering your space.

#### 3. Surveillance cameras

While your workplace probably won't be a crime scene on Law and Order, it's still important to install surveillance cameras on the premises. Surveillance cameras can help deter crime and provide valuable evidence if there is a security breach. They're another easy and invisible tool to help you track who is coming and going in the workplace.

4. Emergency and evacuation plans
Next up, you'll want to have a plan in place for
handling emergency situations. These could be
natural disasters like earthquakes and snow
storms, or external threats like an intruder. Create
a plan with evacuation steps and emergency
contact information.

#### Tip of the month

Bonus tip: With employee scheduling software, you'll be able to know exactly how many employees are onsite. You'll be able to quickly pull that information as well as visitor check-in data to understand how many folks need to be evacuated from the building. Better yet, with seamless integrations, you can send out an emergency message to everyone recorded onsite that day. Talk about streamlined safety!

Cybersecurity best practices
Now that you know your physical workplace is secure,
it's time to look at your digital security. In today's
digital environment, cybersecurity is a major concern
for business. In fact, in 2022, the average cost of a data
breach was \$9.44 million. Let's try to avoid that, shall
we? Here a few office security best practices when it
comes to cybersecurity:

#### 5. Secure passwords

Employees use several platforms and apps to get through their day's work. Keeping track of all those passwords is not only a headache but also a workplace security concern.

Consider investing in a single sign-on tool like Okta that secures all of your login credentials under one main password. This will help keep your employees' passwords secure in one place and limit the possibility of hacking and breaches.

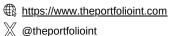
- 6. Regular software updates
  Keeping all of your software and operating
  systems up-to-date can prevent
  vulnerabilities or security breaches. So
  encourage your employees to regularly
  update their laptops. Send out an email or
  Slack reminder and check-in with employees
  who may need extra help.
- 7. Employee training on cyber threats
  Your employees are the most important
  pieces of your security task force. So be sure
  to arm them with helpful tips to stay
  protected. Host regular training sessions on
  topics like password protection or email
  phishing. Schedule them every other month
  and leave room at the end for questions. Your
  employees might catch something that you
  miss
- 8. Unique Wi-Fi credentials
  Visitors, like contractors or business partners,
  might need access to your internet while
  they're onsite. However, granting every guest
  Wi-Fi access can open up the potential for
  security threats. To reduce the risk of
  cyberattacks, contact your IT specialist and
  assign a unique access code to each visitor.
  Doing so will allow you to safely provide
  Internet access to your visitors and not worry
  about any potential risks.

Security Services
Travel Management Services
Logistics

Important links

In Support Of:







When you're at home, you make sure to lock your front door, activate your alarm, and maybe even install a security camera. These practices are important to protect the safety of you, your home, and all of the things and people you care about inside. Well, a workplace is no different. In order to keep everyone and everything inside your workplace safe, you need the right technology, policies, and training in place. Workplace security isn't limited to just the front desk.

It includes the employees and visitors coming in and out of the building, digital and physical assets that live inside, and all confidential information that sits within the four walls of your workplace. So it's important to think holistically about your workplace when you think about securing it. In the following blog post, we'll walk you through a few key features that support modern workplace security. If physical workplace protection is high on your priority list, then follow along with this list of top office security best practices.



Find this interesting?
Why not schedule an appointment with us for more useful security related information.

Email: Nigel Petersen @ nigel@theportfolioint.com or Reshika Tulsie reshika@theportfolioint.com