POST-VISIT PROTOCOLS

- Change passwords, locks, and access controls to rooms, buildings, and computers that long-term visitors used.
- Brief employees on what information can and cannot be shared once the long-term visit or joint venture is completed.
- Educate employees on the policies regarding subsequent contacts from the visitors (the policy may need to provide guidance on contacts via business email, personal email, telephone, in person, social networking sites, etc.); train employees on how to appropriately handle contact with prior visitors.

**Indicators that previous visitors may be trying to obtain restricted information:**

- A prior visitor invites an employee to provide a lecture or receive an award at the visitor’s overseas company.
- An unsolicited email from an associate of a prior visitor requests information or a service that should be directed to another department or person (e.g. sales department).
- Social contact (via email, telephone, social networking sites, or in person) that is inappropriate or manipulative.
- A prior visitor requests favors or additional information.
- A prior visitor requests sensitive information on projects outside the scope of their visit.

**General Guidance**

- Do not leave sensitive information unattended.
- Obtain approval from a supervisor before sharing any sensitive, proprietary, or project information; ensure the recipient is authorized to receive such information.
- If authorized to share sensitive or proprietary information, do not discuss it in an unsecured/open environment.
- Discard sensitive information in a safe manner (e.g. shred).
- Lock computer workstations when unattended.
- Do not store passwords and login instructions at workstations.
- Do not share access codes, user names, or passwords with anyone.
- Do not leave electronic storage devices unattended (external hard drives, thumb drives, laptops etc.).
- Do not allow personal software or hardware (thumb drives) to be installed or attached to company networks without written permission.

If you notice any suspicious behavior or activity, immediately report it to your security officer. Let security determine if an incident is innocent.

For additional information or training, contact the FBI. www.fbi.gov

**Trade Secret** = all types of information (financial, business, scientific, technical, economic, or engineering information including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, codes – whether tangible or intangible) which: (1) the owner has taken reasonable measures to keep secret, and (2) has independent economic value.

**Proprietary Information** = information that is not available to the public, but is not proprietary. It may include information that is export controlled or has publication restrictions.

**Sensitive Information** = information not shared publicly, but is not proprietary. It may include information that is not readily available to them.

---

**Visitors: Risks & Mitigations**

Visitors entering your facility could pose a security risk to your intellectual property or competitive edge. It is an opportunity for competitors to collect information that is not readily available to them.

Some visitors may be trained to verbally elicit information, some may brazenly ignore the security parameters of a tour, and others may use concealed recording devices all in order to obtain restricted information. Some information they collect may seem innocuous, such as the facility layout, but could be very valuable to them and give them clues about your products or how to run their own facility better. Do not tell competitors how to squeeze past you in the economic race, and do not help thieves steal your information.

A visitor played with his wristwatch in a manner that made the host suspicious that a micro camera might be in the watch.
Foreign visitors put double-sided tape on the soles of their shoes in order to collect slivers of metal alloys from the floor of a production plant for US military planes. They later analyzed the slivers to determine the exact metallic components used in the planes.

**SECURITY DURING FACILITY TOURS**

There are a number of commercially available audio and video recording devices disguised as pens, sunglasses, buttons, key fobs, cigarette packs, etc. It may be nearly impossible to keep such devices from entering your facility. Keep this in mind when planning tours.

- Notify visitors of appropriate security and safety
- Ensure visitors are easily identifiable (visitor tours. May be nearly impossible to keep such devices from sunglasses, buttons, key fobs, cigarette packs, etc. It metallic components used in the planes.

**SECURITY DURING LONG-TERM VISITS AND JOINT VENTURES**

Long-term visits or joint ventures may provide an even greater opportunity for a competing company to obtain restricted information. They may also provide an opportunity for visitors to spot, assess, and befriend employees that may assist (either willingly or unwillingly) in collecting restricted information for a visitor during the time of the visit or in the future.

- Provide periodic and sustained reminders on the scope of the project and elicitation detection
- Brief visitors on their obligations and responsibilities including limitations on access or use of computers, copiers, or fax machines, and access limitations to buildings or rooms
- Provide employees with training on how to detect elicitation and recruitment attempts
- Brief employees prior to the arrival of visitors on visitor access limitations, potential collection techniques, economic espionage indicators, and to whom to report security concerns
- Provide employees training on how to detect elicitation and recruitment attempts
- Brief employees prior to the arrival of visitors on visitor access limitations, potential collection techniques, economic espionage indicators, and to whom to report security concerns
- Confront visitors when conducting a security protocol incident
- Refuse to accept unnecessary representatives into the facility
- Do not allow visitors to use networked computers; provide stand-alone computers if needed
- Conduct regular computer audits to detect any efforts by visitors or employees to exceed their approved computer access
- Provide employees with training on how to detect elicitation and recruitment attempts
- Brief employees prior to the arrival of visitors on visitor access limitations, potential collection techniques, economic espionage indicators, and to whom to report security concerns

**Indicators that a visitor may be trying to obtain restricted information during a tour:**

- Make sure employees know when visitors will be in their space and remind them to shield proprietary information from the visitors’ view
- Ensure visitors are easily identifiable (visitor badge, visitor vest, etc.)
- Notify visitors of appropriate security and safety protocols prior to their visit
- Do not hesitate to end the tour and escort visitors out of the facility for non-compliance or other security concerns

**Indicators that a visitor is trying to obtain restricted information:**

- Foreign visitors from a “partnering” university photographed, without approval, every item in another university’s established research lab, to include the make and model of the equipment. The two labs were supposed to be collaborating, but the established lab’s director eventually realized his lab was the only one sharing information.

**Additional Indicators that a Visitor is Trying to Obtain Restricted Information**

- Foreign visitors dipped their ties into chemical solutions in order to obtain samples of the product. They also fanned out in different directions and photographed everything they could in the facility. The host company was subsequently unable to find a market for its product in that country.
- The visitors single out company personnel to elicit information outside the scope of the project
- Visitors want access to the local area network
- Visitors want unrestricted access to the facility
- A visitor faxes or emails documents to an embassy or another country
- A visitor tries to attach an unapproved thumb drive or other device to a computer
- Visitors continually forget security protocols, or need to be reminded “you can’t do that”