# Establishing Security
## After a Wildfire

**In the aftermath of a natural disaster, the security and life safety systems of everything from homes to banks to medical facilities need to be quickly restored to in the recovery. The role of security can become important in identifying scams, organizing security on-site and for any temporary work locations. This should all be accomplished by a trusted worker who understands the importance of protecting company assets and keeping company information confidential.**

**Actions include:**

- Understand the building security procedures and alarm or monitoring systems
- Set up temporary security on-site and temporary locations, if required
- Prevent looting
- Assist those in distress
- Monitor changes in local risks
- Assist emergency crews and any damage assessment teams
- Work with fire and safety officials as required
- Create barricades to dangerous areas on-site
- Determine what, if anything, can be done to prevent further damage to minimize loss of equipment
- Work with restoration providers
- Create procedures to ensure proper access and credentials for anyone on-site or at temporary location(s)
- Identify whether 24-hour security or monitoring is required.
- Work with a security guard company as needed
    - Keep in mind that security staff may need to be transported and supported with food, housing, and rest areas.
    - If new security staff is hired locally, confirm they have been provided the necessary training as well as having had background checks and drug testing.
- Establishing security guard protocols in the event of a secondary evacuation
    - If it is a voluntary evacuation – does security stay?
    - If it is a mandatory evacuation – does the security leave immediately or stay until other staff are out?
- Monitor any inventory or equipment being moved to/from the premises

## Security Coordination for On-Site Operations

- Establish a sign-in/sign-out procedure for contractors and temporary staff. This is also needed for accounting purposes, and should be developed prior to any operations on-site.
- Entry and egress from the site should be through a single designated control site. This site may vary depending upon the damaged area.
- Monitoring contractor work by one or more members on an around the clock basis may be required to prevent additional damage and avoid scams.
- Work to stabilize the facility to the maximum extent possible. This will range from prioritizing areas to sealing building envelopes, to covering of sensitive electronic equipment or garments with waterproof covers.
- Staff should stay within line of sight of others, as much as possible, especially in the early stages of re-entry
- Establish on-site security guards, as needed
- Identify if additional lighting is required
- Do not go anywhere outside of a pre-approved area – even during the day
- Carry a cell phone at all times in case of an emergency.
- Call management and home periodically to let everyone know the situation is still safe enough to remain on-site.
- All staff should keep identification with them.
- Be aware of local restrictions and how to monitor changes to the local situation.
- Prepare for secondary evacuations
- Prepare for those that may experience critical stress by being on-site

## Privacy and Data

- Ensure the area is secure from unauthorized entry
- Identify critical equipment and documents
- Identify whether access to certain areas needs to be restricted
- Identify all outside entities that have access to the location or building.
- Identify contractual privacy needs for any new or temporary location.
- Identify any IT third party risks included in setting up a temporary location. This includes those working in the temporary location, such as:
    - If an existing building's security is used, does a confidentiality clause exist that mentions their security people/company.
    - Does the temporary location's security firm being used have a privacy policy?
    - If an existing building's cleaning staff is used, does a confidentiality clause exist that mentions the cleaning people/company.
- Identify if any staff will bring home any hard copy or electronic records that includes personal information
    - If so, they must be instructed on the appropriate security measures needed – which depends on the level of sensitivity of the data. For instance, any documents containing an individual's health or financial information must have very high security.

## Avoiding Scams

- Con artists are very persuasive and most people naturally let their guard down in the privacy of their own home. You may not think there is anything anyone could say to convince you to give away personal information or credit card numbers, but it happens. There is always the threat of repair scams after a disaster. Be informed about common scams and how to spot them. Here are some examples:
- A contractor asks for a significant portion of money up front, and then disappears, never completing (or even starting) the project.
- A contractor does a fast and faulty repair, like applying used motor oil to "repave" the driveway or painting shingles to make it look like the roof has been repaired.
- A contractor who was "in the neighborhood" points out various items that need repair, often shaming the homeowner into paying for unnecessary or sub-par repairs. Or, he or she offers "free" inspections and then breaks something on purpose in order to get paid to "fix" the problem.
- A pair of contractors knocks on a door and while one creates a distraction, perhaps insisting that he or she look at "damage" outside, while the other sneaks inside and steals anything valuable.
- Do not let an unsolicited contractor inside.
- Ask for a written contract that itemizes the costs and includes a timeline and payment terms of any intended work.
- Never pay in full up front, especially if cash is the only payment accepted.
- Don't be pressured into an on-the-spot decision, even for a discounted price.
- Verify the contractor's references.
- Check for complaints with the Better Business Bureau (BBB).
- Check for reviews about the company online.
- Find out if the company is registered with your state board of contractors and your local building inspection office.
- Make sure the contractor is insured and bonded. (i.e. Require Certificates of Insurance, with Additional Insured endorsements for any contractors or service providers performing work on the site).
- If a utility worker requests access to your home without prior notice, verify his or her identity with the utility company before letting the worker inside.
- Be aware of look-alike charities. Watch out for charities with similar names to well-known organizations. Some scam artists try to trick people by using names that make them appear to be the same as or comparable to valid charities.
- Be aware of contribution collectors. Stay cautious of charities that offer to send a representative to collect donations.
- Be aware of charity related email scams. Be skeptical of emails seeking charitable contributions. Many unsolicited messages received through email are fraudulent.
- Be aware of adamant demands for a supposed charitable organization. Refuse any high-pressure requests for your contribution. Legitimate charities usually don't require people to give at a moment's notice.

**CONTACT YOUR LOCAL HUB** for additional risk management resources and advisement for your business.

For even more information, visit www.hubinternational.com