Contractor Management Manual

Prepared for HIROC Subscribers

Health care Insurance Reciprocal of Canada

Version 1.0—February 2021

HIROC – Contractor Management Manual

Table of Contents

Introduction

FM Global has partnered with HIROC with the goal of minimizing the potential for, and severity of property losses taking place within healthcare facilities. The purpose of this Manual is a high-level overview of property loss prevention guidelines that contractors should follow to ensure a safe environment for all parties involved, including patients, staff, and visitors. This is a critical part of a good property conservation program, which is defined as a managed and organized effort aimed at eliminating and/or minimizing the potential for loss through both physical protection and improved operating practices.

Each contractor company must thoroughly review their own work practices and workplace hazards, providing employees all the necessary training and equipment for their safety. Companies are responsible for ensuring that proper workplace safety is followed by their employees and/or sub-contractors, while they are working at the subscriber facilities. All required training should be completed prior to the contractor employee attending the facility. In no way does this manual include all the safety issues or concerns one may encounter on a given day. All contractors/vendors are expected to abide by all codes, regulations, and standards as applicable to their trade and scope of work set out by the authority having jurisdiction.

The sections below will review some areas of property loss prevention that a contractor should follow to protect your facilities. These areas are outlined as:

1. Site Access and Security
2. Hot Work Management, including Torch-Applied Roofing
3. Fire Protection Impairments
4. Smoking
5. Housekeeping
6. Hazardous Materials and Processes
7. Other Policies and Procedures
8. Training
9. Resources

Additional training on the programs outlined below can be found at the following website and registering using the account number **54887**: https://fmglobaltraining.skillport.com/.

Please feel free to reach out to your dedicated representatives for FM Global and HIROC with any questions:

FM Global
Shiva Nourmansouri, P.Eng.
Account Engineer
shiva.nourmansouri@fmglobal.com
(905) 763-5586

HIROC
Jean Asuncion, CIP, CRM
Engineering Liaison Associate
jasuncion@hiroc.com
(416) 730-3015

1.0 Site Access and Security

Healthcare facilities are particularly vulnerable to unauthorized access because they are designed to be publicly accessible even though they contain a high concentration of valuable information, contents, materials, and equipment. Threat actors want to gain unauthorized entry into facilities for numerous reasons, including financial gain and malicious intent. Recently, accessing a facility's network has become a prominent motive in itself.

Each facility should conduct a complete security risk assessment to identify any vulnerabilities. Create and maintain a documented physical/cyber security program to manage your contractors against the identified vulnerabilities. This should include an incident response plan to follow when unauthorized access of various kinds has been detected. This program should be tested regularly, and employees should be trained in security awareness. Some of the key items to consider are listed below, however, each security program should be customized to the facility's needs and include additional detail.

1. Instructions for logging in when contractors arrive on site, including method to track whereabouts of all contractors should be recorded while on site (i.e. identification badge). Contractors should be escorted until physical security measures have been implemented.
2. A knowledgeable employee should be assigned to oversee the contractors, understand their scope of work, monitor work quality, and check for procedural violations.
3. Develop a map for designated security levels at your facility. It should be confirmed that all server rooms and sensitive areas are adequately locked. Access to these secured/sensitive areas should be controlled for the contractor (i.e. screening, logging, badging, no "tailgating" policy, etc.). After-hours contractors should be escorted while on the property.
4. Implement strict controls over the use of portable media and devices. Contractors who require access to the production network should be provided with the ability to access only those specific systems, applications, and/or network segments required to perform their contracted responsibilities. Contractor company must follow procedures to ensure using computers or other portable media devices (USB drives) to service equipment do not introduce a cyber risk (i.e. malware, viruses) to the information technology network.

All contractors should be provided with a security briefing and explanation of the security program. The security program guidelines should be provided in the contract for work.

Ensure training on all the programs in this manual has been received prior to contactor sign-in. The identification badges worn by contractors or other forms of documentation should be used as compliance with the training requirements. Identification badges should not be worn until required training is completed. Identification badges should always be worn while on site.

Resources: FM Global Property Loss Prevention Data Sheet 9-1, *Supervision of Property*
FM Global Property Loss Prevention Data Sheet 10-4, *Contractor Management*
Understanding the Hazard - *Physical Security: Unauthorized Access* (Appendix A)

2.0 Hot Work Management

Fires and/or explosions caused by hot work or conditions that may lead to these hazardous events should not be tolerated at your facilities. Implement a Hot Work Policy for all hot work activities at your existing facilities or new construction sites. The policy should mandate thorough and effective hot work procedures which describes a mandatory, supervised, step-by-step, hot work permit system and applies to all employees and contractors.

It should be mandated that contractors should be in possession of an approved Hot Work Permit before hot work begins. The first step is to ensure alternatives to hot work are always considered and encouraged (i.e. cold work options). Contractors hired to do work potentially involving hot work must comply with all requirements of the hot work permitting process and should be overseen by a designated facilities employee.

The FM Global Hot Work Permit outlines the key items to consider in mitigating the hazards associated with hot work. See Appendix B for a sample copy of the FM Global Hot Work Permit.

Some of the key steps of the FM Global Hot Work Permit System include:

1. Prohibit hot work where conditions are severe beyond correction (i.e. lint or dust accumulations or presence of flammable liquids/vapours).
2. Available fire protection is verified to be in service and operable.
3. The 35-foot rule (10 m): Keep combustible materials at least 35 ft (10m) away from the hot work. Use FM Approved blankets, weld pads, or curtains to cover any combustible construction and/or nonremovable combustibles within a 35 ft radius.
4. Enforce all job-specific precautions as listed on the Hot Work Permit. Notify FM Global and/or HIROC if you have any questions about hot work activity.
5. Issue Part 2 of the Hot Work Permit to the person doing the job.
6. Ensure fire watch is provided during and for 60 minutes after work. Hot work should be monitored for 3 additional hours after hot work has been completed (unless your FM Global engineer has provided an exception to the monitoring period based on the risk matrix).
7. Keep Part 2 on file for future reference, including signed confirmation that the post-work fire watch and monitoring have been completed.
8. Sign off the final check on Part 2 of the Hot Work Permit. Keep records for review by management and FM Global.

All personnel involved in the hot work policy procedure, including facilities staff, contractors or subcontractors should complete the FM Global Hot Work training on the FM Global Training website and present a certification of completion prior to the start of the work:
https://training.fmglobal.com/

Resources: FM Global Property Loss Prevention Data Sheet 10-3, *Hot Work Management*

2.1 Torch-Applied Roofing

Installing torch-applied roof (TAR) systems is a common cause of construction fires. Additional design considerations and precautions should be taken during the installation of TAR systems for new roof construction, re-roofing, recovers, altering, or repairing roof systems.

Treat work on torch-applied roofing systems as a hot work high-risk operation. Torch-applied roofing includes modified bitumen roof covers using an open-flame roofer's torch. In general, these types of roofs are more likely to cause a fire than a roof installation that uses fasteners and adhesives. This is particularly true where a new roof is being installed on an existing building that already has combustible materials in the construction and occupancy.

When using torch-applied roofing systems, follow the strict hot work policy per Section 2.0, guidelines of the roofing system manufacturer, and take additional required precautions per FM Global Data Sheet 1-33, *Safeguarding Torch-Applied Roof Installations*.

Some of the key points to consider are:

1. Develop a roof-fire emergency response plan that includes conditions under which the fire service should be notified and verify the fire service has access to the work area.
2. Use additional caution when working around roof openings, penetrations, or flashings.
3. Follow the manufacturer's instructions for the use of torches to secure roofing membranes. Constantly move the flame from hand-held torches from side to side. If a mobile heating apparatus is used, keep it in constant motion while operating.
4. Heat the exposed outer surface of the membrane roll until a slight sheen develops. Do not overheat the membrane as this could cause smoldering or ignition of it, which is evidenced by a slight smoke vapor.
5. Use a torch stand to direct the flame upward when momentarily not in use. Close the cylinder valve to burn off propane in the line before shutting off the torch head. Shut off the gas supply whenever a propane odor (rotten egg smell) is detected.
6. Do not use torches near gas lines, electrical wires, or ignitable liquids.
7. Use only FM Approved assemblies as detailed in Roof*Nav*. Do not apply the torch flame to combustible substrates (such as foam plastic, kraft-faced glass fiber, wood fiber insulation or cant strips, or plastic fastener plates) when installing the membrane. Do not allow torch flames to encounter adhesives other than those in the TAR itself.
8. Do not install torch-applied roofing during high wind conditions (when wind speed is faster than 10 mph (4.5 m/s).
9. Do not store other combustible materials (apart from propane cylinders; see Section 2.2.6) within 35 ft (11 m) of areas in which torches will be used. This includes, but is not limited to, stored insulation, roof covering, and solvents.

Resources: FM Global Data Sheet 1-33, *Safeguarding Torch-Applied Roof Installations*
https://roofnav.fmglobal.com

3.0 Impairment Management (Red Tag Permit System)

Each facility should implement an impairment management program to ensure that any time a sprinkler control valve is shut or a fire pump controller is turned to the "off" position, the appropriate personnel are notified and the system is returned to service once the impairment is no longer needed. The FM Global Red Tag Permit System can be used at your facilities and outlines key precautions to take before, during and after an impairment takes place.

The facility impairment policy should state that before the start of any work on the fire protection system, contractors should be responsible to notify the facility's assigned employee of the scope of work and if any fire protection valves/systems will be impaired. The contractor must be in possession of an approved Red Tag Permit provided by a facility employee prior to the start of any work. This includes all planned and emergency situations.

The contractor should be fully trained on their role in the Fire Protection Impairment Policy and have a full understanding of procedures and guidelines well before the start of any work on the fire protection system. Some of the key steps include:

1. Management fills out, signs, and issues the Red Tag Permit, describing the location of the facility, the reason for impairment, and the planned duration of the impairment.
2. Notify FM Global at 1-800-955-3632 of the impairment. Alternatively, fill out the Red Tag Permit online using www.fmglobal.com/redetag. (Refer to Appendix C for a sample copy).
3. During the impairment:

a. place Part 2 of the Red Tag in the center pocket of the Wall Kit as a visual reminder of the impairment.
b. Issue Part 3 of the Red Tag to the Fire Protection Equipment Operator to attach to the impaired valve.
c. Take the necessary precautions. Eliminate ignition sources. Enforce the “no hot work” rule.
d. Assign a fire watch to patrol the area where protection is down.
e. Work without interruption.

4. After work is completed, restore fire protection to service and contact FM Global Customer Service Desk 1-800-955-3632 or reply to the auto-generated email from Online Red e-Tag in your inbox if submitted electronically to close the impairment. Lock fire protection control valves in the wide-open position.

Figure 1: FM Global Red Tag Permit System

All personnel involved in the fire protection impairment policy procedure, including facilities staff, contractors or subcontractors should complete the FM Global Red Tag Permit System training on the FM Global Training website and present a certification of completion prior to the start of the work: https://training.fmglobal.com/

4.0 Smoking Policy

A smoking policy should be developed, and all smoking in any form (cigarettes, cigars, smokeless tobacco, e-cigarettes etc.) should be prohibited in all areas of the facility, specifically areas where there are combustibles or storage, where ignitable liquids are stored or dispensed, near piles of debris, and on the roof. For contractors, this should include the project site, new construction sites, and may include adjacent public sidewalks and rights-of-way as designated by the facilities manager.

Your site’s smoking policy should be fully reviewed with all contractors.

5.0 Housekeeping

A housekeeping policy should be developed to ensure all construction work sites are always kept clean and free of trash, rubbish, construction debris, scrap, or miscellaneous materials that should also not be permitted to accumulate. Key items in a housekeeping policy could include:

1. The contractor should clear and sweep the work site, during and at the end of each shift. Rubbish, scrap, and other materials shall be disposed of in contractor supplied containers which are code compliant. The facilities manager or project manager should be assigned to regularly check the contractor's work site.
2. Electrical rooms and server/computer rooms should be kept free of storage. Signage should be used to maintain this policy.
3. Ignitable liquid or hazardous material spills should be cleaned up immediately. Proper material-handling procedures should be taken by all contractors.
4. There should be no obstacles blocking the fire doors. This could prevent the doors from shutting in the event of a fire, which would allow fire spread throughout the building.
5. Include a formal system for employees to report potential problems.

Overall, good housekeeping practices sets the tone for all property loss prevention efforts.

6.0 Hazardous Materials and Processes

Hazardous materials and policies should be developed for outside contractors. Facilities management and contractors should all be made aware of the presence and location of all hazardous material, including special handling instructions. The following key items can be considered:

1. Any hazardous chemicals brought on site by an outside contractor should be pre-approved. The use of hazardous materials should be minimized, and efforts should be made such that the contractor have no more than one day's use of a hazardous material stored as required. All hazardous materials should be removed immediately upon use and not stored on site for more than 5 days of non-use. If required and applicable, FM Approved ignitable liquid cabinet should be used to store the materials.
2. Prior to any chemical or agent being brought on site the contractor must provide the Safety Department, Facilities Operations Manager and Project Manager a list of all materials to be used and the appropriate SDS. All contractors must keep copies of SDS's on site for all chemicals and hazardous substances to be used on the job, including lubricants, solvents, paints, etc. All chemicals shall be properly labeled.
3. No chemical shall be used that generates a fume in the process, without prior approval from the facility Safety Department, Project Manager and Facilities Operations Department.
4. Contractors are responsible for ensuring their employees are properly trained with any chemical, or agent prior to such agents being brought on site. Chemicals shall be maintained within the contractor's control. Chemicals brought in by the contractor shall be kept out of the control of team members, patients, visitors, and other persons who are not trained in that specific chemical.
5. Contractors shall have a written spill response plan for all chemicals that are brought on site. Contractors shall have the appropriate materials and apparatus (spill kit) to control and minimize any spill of a chemical in their area. Each contractor must establish and maintain an effective hazard communication program.

6. Refer to the facility's Emergency Procedures for Spilled Chemicals document. If material that contains asbestos or other hazardous material is suspected or encountered, stop work immediately, notify the Project Manager or Facilities Operations Manager, and proceed only after conditions are verified and a mitigation plan has been approved.

7.0 Other Policies & Procedures

Contractor management should be incorporated into other policies and procedures as indicated below. The contractors should be made aware of all practices and procedures pertaining to their presence at your facilities and should be trained on all of these items. In addition to the above topics, the following items should be discussed and reviewed with the contractors:

1. Reporting incidents and property damage
2. Prevention of Freeze-Ups (FM Global Property Loss Prevention Data Sheet 9-18, *Prevention of Freeze-Ups*)
3. Safeguards for the use of Temporary Heaters
4. Emergencies (fire, water, natural hazards, etc.- FM Global Property Loss Prevention Data Sheet 10-2, *Emergency Response*)
5. Environmental protection
6. Lockout /tag out of equipment
7. Electrical isolation procedures and best practices
8. Specific training on tools/equipment while on site
9. Excavation and trenching (ensure contractor's regrading does not expose the site to potential storm water damage, ensure all mains are identified to reduce risk of puncture during excavation practices, etc.)

8.0 Training

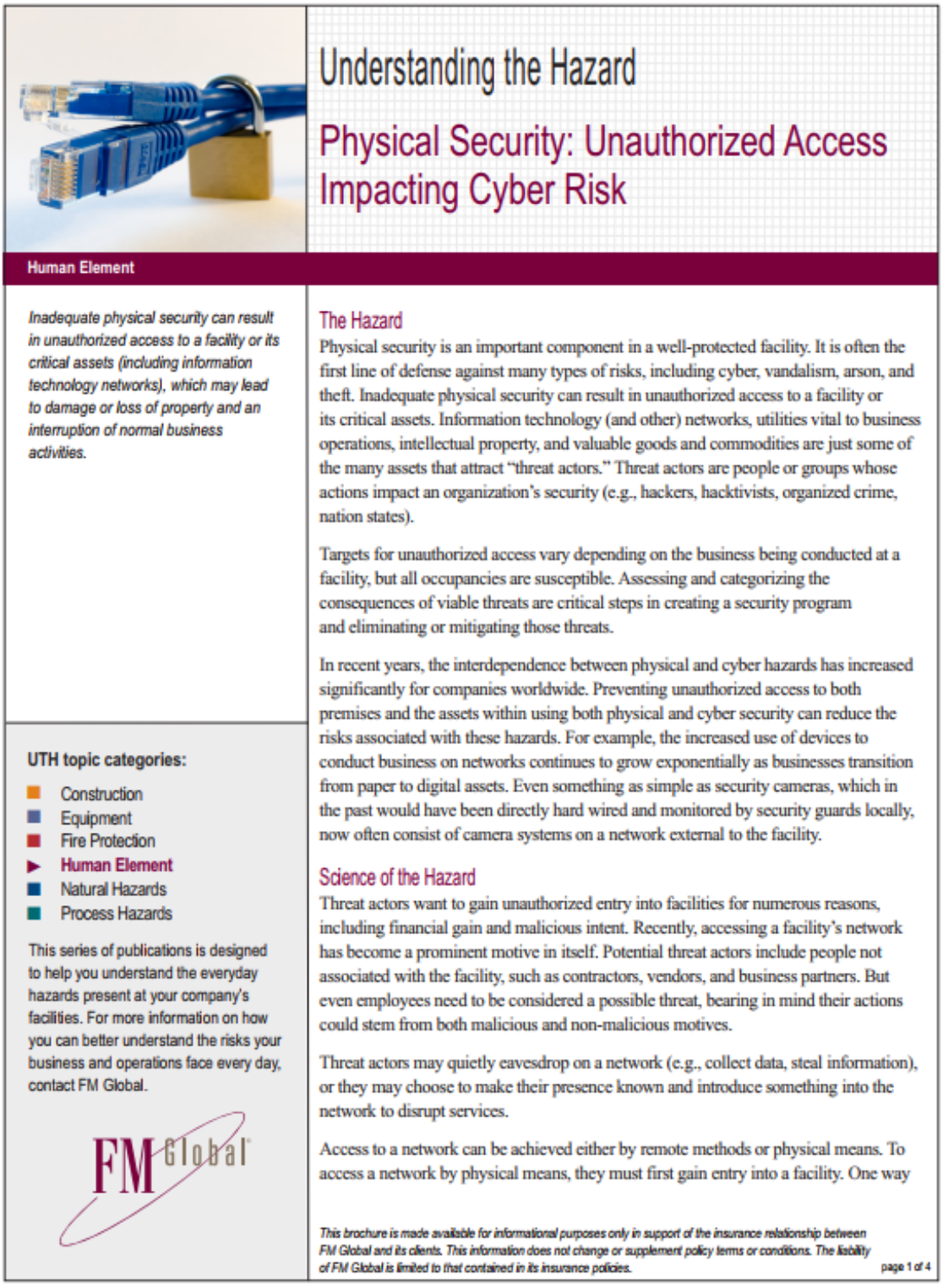
Prior to working at any of your facilities, the contractors should be required to receive training on all applicable policies and procedures referenced in this manual. This training should be required to be completed on a minimal annual basis. The contractor provider shall maintain current readily available records of all training prescribed in this manual. Training records shall include the Certificate of Completion for the training issued to each personnel. Training records shall be auditable by the facilities management without prior notice.

FM Global training on the programs can be found at the following website and registering using the account number **54887**: https://fmglobaltraining.skillport.com/.

9.0 Resources

- FM Global Property Loss Prevention Data Sheets: www.fmglobaldatasheets.com/
- FM Global Loss Prevention Training: https://fmglobaltraining.skillport.com
- FM Approved products: https://www.approvalguide.com/
- FM Global catalog for free resources: https://fmglobalcatalog.com/
- RoofNav: https://roofnav.fmglobal.com

Appendix A: Physical Security: Unauthorized Access Impacting Cyber Risk



Understanding the Hazard

Physical Security: Unauthorized Access Impacting Cyber Risk

Human Element

Inadequate physical security can result in unauthorized access to a facility or its critical assets (including information technology networks), which may lead to damage or loss of property and an interruption of normal business activities.

UTH topic categories:

- Construction
- Equipment
- Fire Protection
- ▶ Human Element
- Natural Hazards
- Process Hazards

This series of publications is designed to help you understand the everyday hazards present at your company's facilities. For more information on how you can better understand the risks your business and operations face every day, contact FM Global.

FM Global

The Hazard

Physical security is an important component in a well-protected facility. It is often the first line of defense against many types of risks, including cyber, vandalism, arson, and theft. Inadequate physical security can result in unauthorized access to a facility or its critical assets. Information technology (and other) networks, utilities vital to business operations, intellectual property, and valuable goods and commodities are just some of the many assets that attract "threat actors." Threat actors are people or groups whose actions impact an organization's security (e.g., hackers, hacktivists, organized crime, nation states).

Targets for unauthorized access vary depending on the business being conducted at a facility, but all occupancies are susceptible. Assessing and categorizing the consequences of viable threats are critical steps in creating a security program and eliminating or mitigating those threats.

In recent years, the interdependence between physical and cyber hazards has increased significantly for companies worldwide. Preventing unauthorized access to both premises and the assets within using both physical and cyber security can reduce the risks associated with these hazards. For example, the increased use of devices to conduct business on networks continues to grow exponentially as businesses transition from paper to digital assets. Even something as simple as security cameras, which in the past would have been directly hard wired and monitored by security guards locally, now often consist of camera systems on a network external to the facility.

Science of the Hazard

Threat actors want to gain unauthorized entry into facilities for numerous reasons, including financial gain and malicious intent. Recently, accessing a facility's network has become a prominent motive in itself. Potential threat actors include people not associated with the facility, such as contractors, vendors, and business partners. But even employees need to be considered a possible threat, bearing in mind their actions could stem from both malicious and non-malicious motives.

Threat actors may quietly eavesdrop on a network (e.g., collect data, steal information), or they may choose to make their presence known and introduce something into the network to disrupt services.

Access to a network can be achieved either by remote methods or physical means. To access a network by physical means, they must first gain entry into a facility. One way

Figure 2: Physical Security UTH

What You Can Do at Your Facility

Now:

- Lock doors and secure sensitive areas.
- Establish procedures for employee, visitor, and contractor access. Have visitors and contractors escorted until you have physical security measures in place.
- Implement strict controls over the use of portable media and devices, such as flash drives, CDs, and laptops that are used to interface with the production network.
- Conduct a physical security risk assessment at your facility to identify vulnerabilities.

Soon:

- Create and maintain a documented physical security program, and test it regularly.
- Separate your guest network from your production network and password protect it.
- Integrate your security program across all applicable groups: Facilities, IT, Risk Management, etc.
- Develop a physical security incident response plan to follow when unauthorized access of various kinds has been detected.
- Train employees in security awareness.

of doing this is called "social engineering," a type of psychological manipulation used to get people to unwittingly perform an action or divulge confidential information. Examples include posing as a conscientious contractor who needs access to complete his work, a friendly vendor who has forgotten her keycard, or an engaging stranger laden with packages for whom you politely hold open the door. Threat actors may also sneak in through poor perimeter or building security during or after business hours.

Once inside the facility, they may connect to the network using various means, including the following:

- Unlocked server rooms, unsecured server cabinets.
- Unattended employee computers or workstations (leaving a computer unlocked is equivalent to leaving a note with the password written on it).
- A junction into a network cable.
- Network ports (e.g., on wall outlets). Threat actors can plug their own router or Wi-Fi device into a network port that they can later tap into, creating their own "backdoor" outlet (analogous to unlocking a back door that can be opened later), or introducing malware into the network.
- Wi-Fi/wireless network access. Depending on the Wi-Fi footprint, a threat actor doesn't even need to be inside the building to obtain access. They could be sitting in a car in the parking lot. This is why having a separate guest network is much safer than having one firewalled from the production network. With a firewall, a physical bridge to the production network still exists, and there are ways to cross that bridge.

Loss Experience

In 2014, employee workstations inside a large entertainment company were hijacked. Reportedly, the threat actors, who were advocating for social equality rather than financial gain, were given physical access to the building by sympathetic employees. They were allowed to move around without an escort, and administrative computers were logged in and left unattended. The hijackers stole the computer credentials of a system administrator, which gave them broad access to the company's computer systems. Once on the network they planted malware, wiping out half of the company's global network. Among the items reportedly compromised were private key files: source codes, passwords for corporate databases, inventory lists of hardware and other assets, production outlines and templates, as well as production schedules and notes. As a result, the company had to completely sever their network from the Internet. Prior to isolating their network, however, the malware used algorithms to erase files, preventing recovery and corrupting the startup software for each computer. In addition, confidential information was published on public file-sharing sites.

In 2011, an international pharmaceutical company experienced an attack that shut down their operations for several days because they were unable to process checks, ship products, or communicate by email. It cost them at least US$300,000 to respond to the attack, conduct damage assessments, and restore the company's network. The attack was initiated by a former IT employee. After learning that company layoffs would affect a friend, the ex-employee, who had resigned several months earlier, used administrative passwords (which had not been changed since he left the company) to gain access to the company's network. He then installed software that deleted dozens of virtual servers that housed most of the company's North American computer infrastructure.

Figure 3: Physical Security UTH (continued)

Definitions

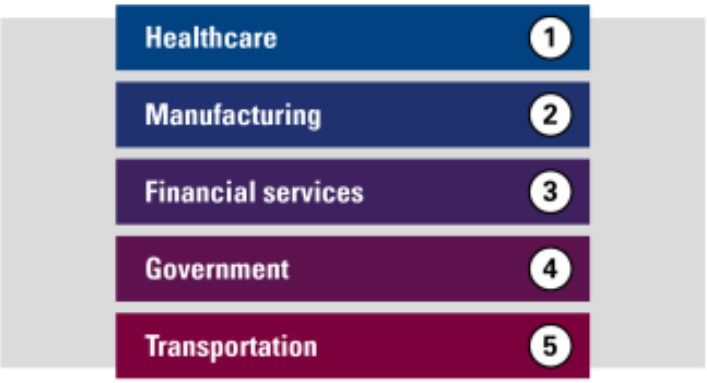
Risk assessment: A process of identifying internal and external security threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical function necessary to continue operations, and defining the controls in place or necessary to reduce the exposure.

Security vulnerability assessment (SVA): A systematic and methodical analysis in which an occupancy's security vulnerabilities are identified, quantified, and prioritized to prevent an undesired outcome.

Threat actor: An entity (e.g., hacker, hacktivist, insider threat, nation state, organized crime) that is partially or wholly responsible for an incident that impacts an organization's security.

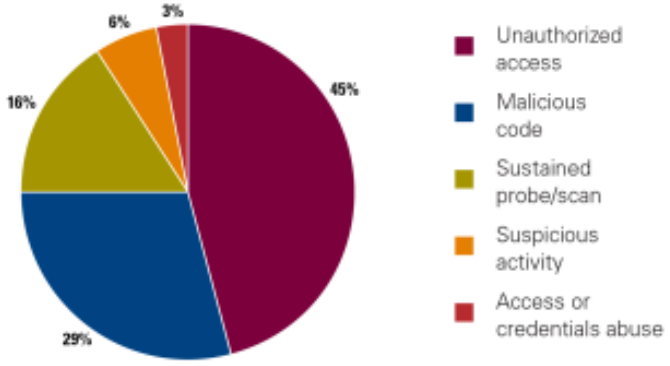
The charts below show the industries with the highest incidence of cyber attack in 2015, and the most frequently occurring incidents for those industries, according to a 2016 report by IBM Security, "Reviewing a Year of Serious Data Breaches, Major Attacks and New Vulnerabilities."

Industries with the Highest Incidence of Cyber Attack, 2015



Source: IBM Security

Most Frequently Occurring Incidents, 2015



Source: IBM Security

But What About...

...the fact my facility is not a data center or a healthcare facility? Do I really need to consider physical security from a cyber risk perspective?

All occupancies are susceptible to cyber risk from a physical security breach. Threat actors often go after the "weakest link," exploiting the fact that many facilities have less than robust physical security programs because they do not believe themselves to be a target. It's a myth that only data centers and healthcare facilities should be concerned about this risk. In fact, other types of facilities (e.g., manufacturing) are increasingly becoming targets.

Figure 4: Physical Security UTH (continued)

Need More Information?

Ask your FM Global engineer or client service team about the following:

- FM Global Property Loss Prevention Data Sheet 9-1, *Supervision of Property*
- FM Global publication *Understanding the Hazard: Cyber Attacks* (P16177)

...the fact our guest Wi-Fi network is separate from our production network? Why do I need to password protect it?

Just as you wouldn't want strangers going into your house without your knowledge, it is a good idea to only have known guests logging into your network for the following reasons:

- To reduce the threat of someone "listening in" on your network and collecting proprietary information.
- If people commit cyber crimes using an Internet line or network associated with your business, it could negatively impact your reputation.
- Knowing who is on your network gives you a better chance of identifying a culprit if anything goes wrong.
- It is important to provide a secure network for trusted people (clients, business associates, etc.) who may need to transmit sensitive information.

...the fact we often have contractors at our facility that service equipment using their own computers or devices? How can I ensure they are not introducing a cyber risk to our network?

Do not allow contractors to plug their computer directly into your network. Their computer or device could be infected and introduce malware onto your network. Provide the contractor with a non-network computer to do their work on. If this is not possible (e.g., the contractor is servicing equipment using proprietary software), scan or test the contractor's computer or device before allowing it to connect to your production network.

Don't Let This Happen To You

Leaving a computer unlocked is equivalent to leaving a note with your password written on it.

Ordering Information
For additional copies of Understanding the Hazard publications, contact your FM Global engineer or client service team.

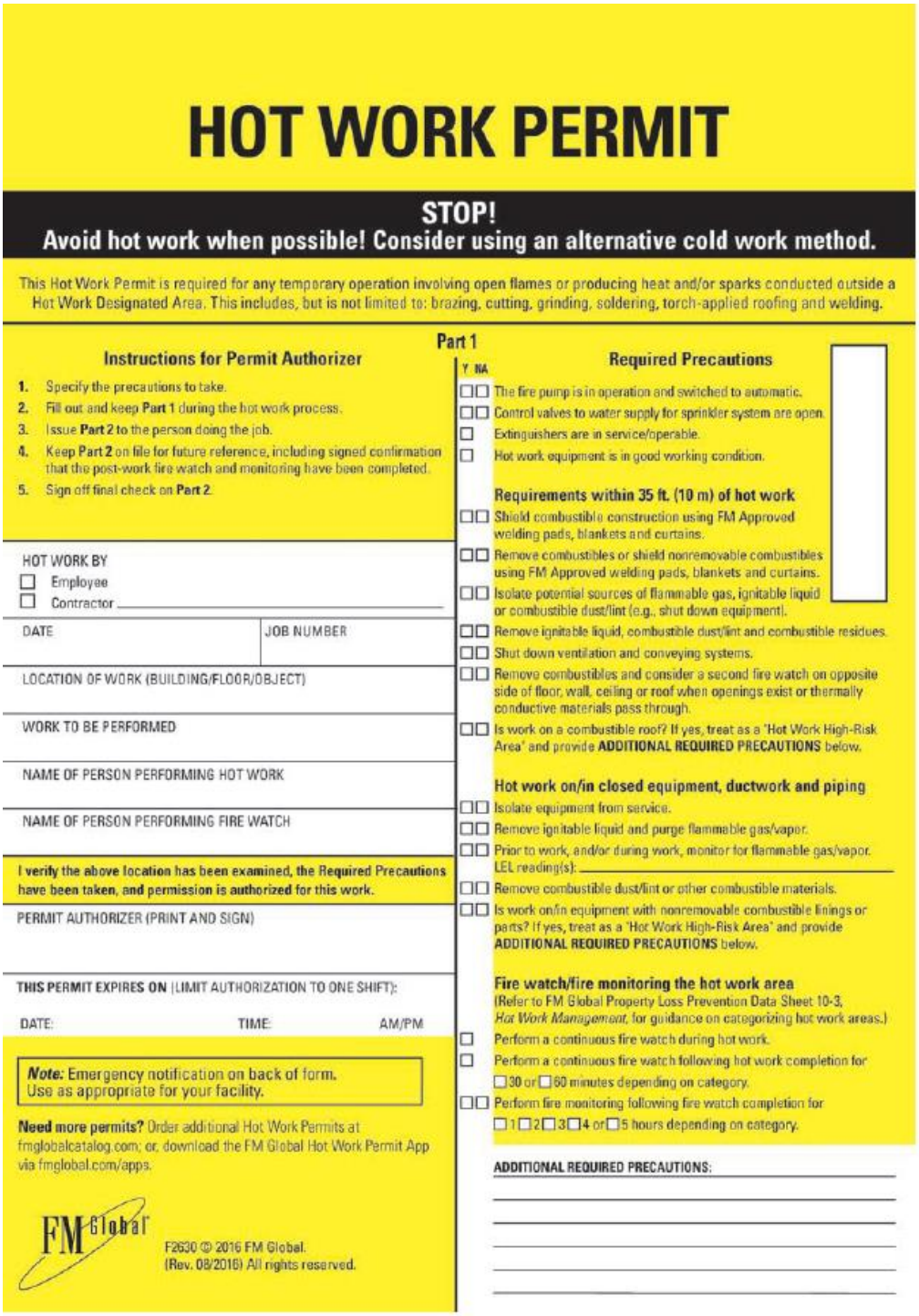
Additional FM Global brochures and educational material can be found in the FM Global Resource Catalog and ordered or downloaded online at www.fmglobalcatalog.com. Or, for personal assistance worldwide, contact our U.S.-based customer services team, Monday – Friday, 8 a.m. – 5 p.m. ET :

- Toll-free: (1)877 364 6726 (Canada and United States)
- By phone: +1 (1)401 477 7744
- By fax: +1 (1)401 477 7010
- E-mail: customerservices@fmglobal.com

Figure 5: Physical Security UTH (continued)

Appendix B: Hot Work Permit

Hot work permits and wall kits can be ordered through the FM Global Resource Catalog at http://www.fmglobalcatalog.com or toll free at 1-877-364-6726.



HOT WORK PERMIT

STOP!
Avoid hot work when possible! Consider using an alternative cold work method.

This Hot Work Permit is required for any temporary operation involving open flames or producing heat and/or sparks conducted outside a Hot Work Designated Area. This includes, but is not limited to: brazing, cutting, grinding, soldering, torch-applied roofing and welding.

Part 1

Instructions for Permit Authorizer

1. Specify the precautions to take.
2. Fill out and keep **Part 1** during the hot work process.
3. Issue **Part 2** to the person doing the job.
4. Keep **Part 2** on file for future reference, including signed confirmation that the post-work fire watch and monitoring have been completed.
5. Sign off final check on **Part 2**.

HOT WORK BY
☐ Employee
☐ Contractor _____

DATE | JOB NUMBER

LOCATION OF WORK (BUILDING/FLOOR/OBJECT)

WORK TO BE PERFORMED

NAME OF PERSON PERFORMING HOT WORK

NAME OF PERSON PERFORMING FIRE WATCH

I verify the above location has been examined, the Required Precautions have been taken, and permission is authorized for this work.

PERMIT AUTHORIZER (PRINT AND SIGN)

THIS PERMIT EXPIRES ON (LIMIT AUTHORIZATION TO ONE SHIFT):

DATE: TIME: AM/PM

Note: Emergency notification on back of form. Use as appropriate for your facility.

Need more permits? Order additional Hot Work Permits at fmglobalcatalog.com; or, download the FM Global Hot Work Permit App via fmglobal.com/apps.

FM Global

Required Precautions

Y NA

☐☐ The fire pump is in operation and switched to automatic.
☐☐ Control valves to water supply for sprinkler system are open.
☐ Extinguishers are in service/operable.
☐ Hot work equipment is in good working condition.

Requirements within 35 ft. (10 m) of hot work

☐☐ Shield combustible construction using FM Approved welding pads, blankets and curtains.
☐☐ Remove combustibles or shield nonremovable combustibles using FM Approved welding pads, blankets and curtains.
☐☐ Isolate potential sources of flammable gas, ignitable liquid or combustible dust/lint (e.g., shut down equipment).
☐☐ Remove ignitable liquid, combustible dust/lint and combustible residues.
☐☐ Shut down ventilation and conveying systems.
☐☐ Remove combustibles and consider a second fire watch on opposite side of floor, wall, ceiling or roof when openings exist or thermally conductive materials pass through.
☐☐ Is work on a combustible roof? If yes, treat as a "Hot Work High-Risk Area" and provide **ADDITIONAL REQUIRED PRECAUTIONS** below.

Hot work on/in closed equipment, ductwork and piping

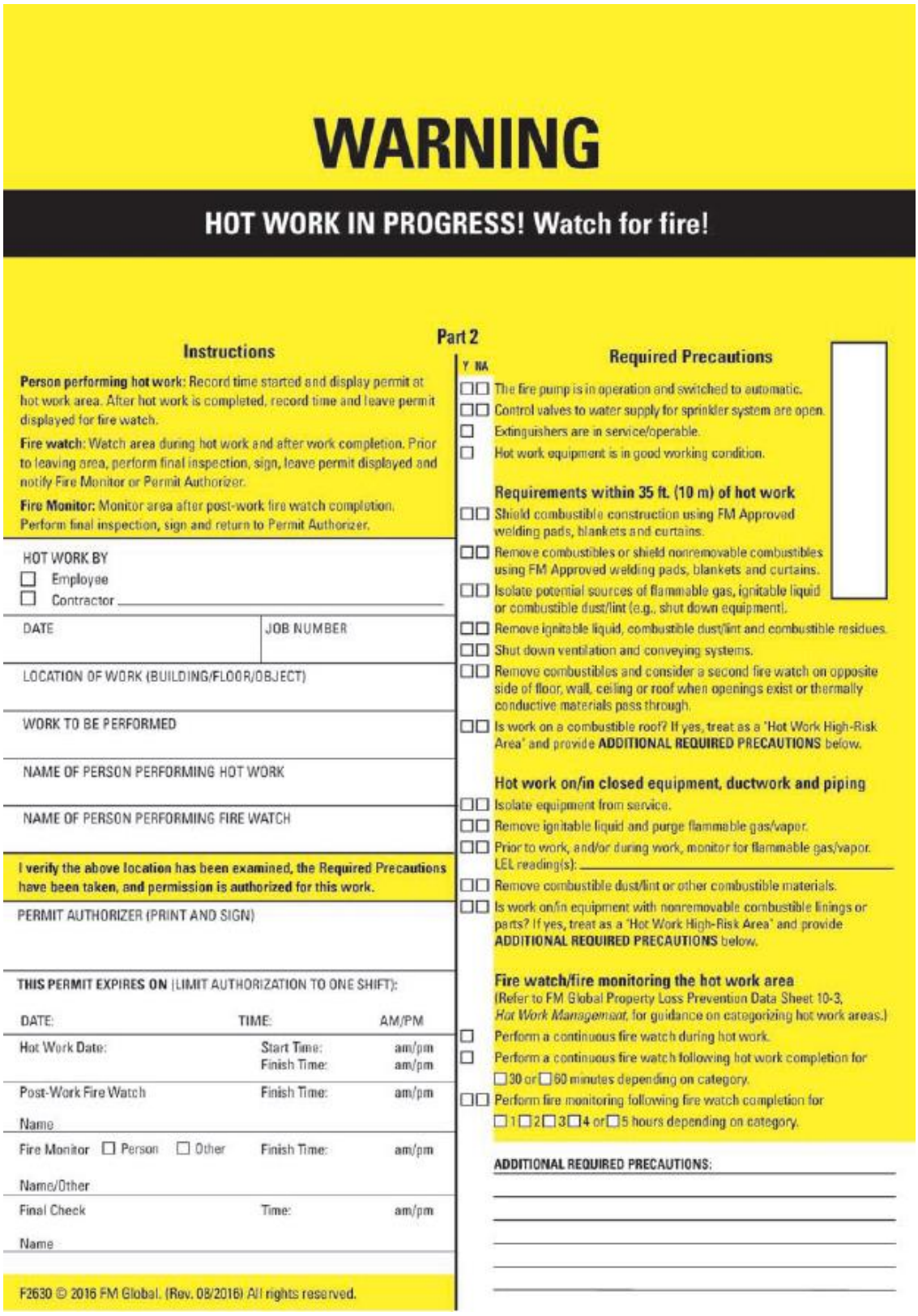
☐☐ Isolate equipment from service.
☐☐ Remove ignitable liquid and purge flammable gas/vapor.
☐☐ Prior to work, and/or during work, monitor for flammable gas/vapor. LEL reading(s): _____
☐☐ Remove combustible dust/lint or other combustible materials.
☐☐ Is work on/in equipment with nonremovable combustible linings or parts? If yes, treat as a "Hot Work High-Risk Area" and provide **ADDITIONAL REQUIRED PRECAUTIONS** below.

Fire watch/fire monitoring the hot work area
(Refer to FM Global Property Loss Prevention Data Sheet 10-3, *Hot Work Management*, for guidance on categorizing hot work areas.)

☐ Perform a continuous fire watch during hot work.
☐ Perform a continuous fire watch following hot work completion for ☐30 or ☐60 minutes depending on category.
☐☐ Perform fire monitoring following fire watch completion for ☐1 ☐2 ☐3 ☐4 or ☐5 hours depending on category.

ADDITIONAL REQUIRED PRECAUTIONS:

Figure 6: Hot work permit (front view)



WARNING

HOT WORK IN PROGRESS! Watch for fire!

Instructions

Person performing hot work: Record time started and display permit at hot work area. After hot work is completed, record time and leave permit displayed for fire watch.

Fire watch: Watch area during hot work and after work completion. Prior to leaving area, perform final inspection, sign, leave permit displayed and notify Fire Monitor or Permit Authorizer.

Fire Monitor: Monitor area after post-work fire watch completion. Perform final inspection, sign and return to Permit Authorizer.

HOT WORK BY
☐ Employee
☐ Contractor _____

DATE | JOB NUMBER

LOCATION OF WORK (BUILDING/FLOOR/OBJECT)

WORK TO BE PERFORMED

NAME OF PERSON PERFORMING HOT WORK

NAME OF PERSON PERFORMING FIRE WATCH

I verify the above location has been examined, the Required Precautions have been taken, and permission is authorized for this work.

PERMIT AUTHORIZER (PRINT AND SIGN)

THIS PERMIT EXPIRES ON (LIMIT AUTHORIZATION TO ONE SHIFT):

DATE:	TIME:	AM/PM
Hot Work Date:	Start Time: Finish Time:	am/pm am/pm
Post-Work Fire Watch Name	Finish Time:	am/pm
Fire Monitor ☐ Person ☐ Other Name/Other	Finish Time:	am/pm
Final Check Name	Time:	am/pm

F2630 © 2016 FM Global. (Rev. 08/2016) All rights reserved.

Part 2

Required Precautions

Y NA

☐☐ The fire pump is in operation and switched to automatic.
☐☐ Control valves to water supply for sprinkler system are open.
☐ Extinguishers are in service/operable.
☐ Hot work equipment is in good working condition.

Requirements within 35 ft. (10 m) of hot work

☐☐ Shield combustible construction using FM Approved welding pads, blankets and curtains.
☐☐ Remove combustibles or shield nonremovable combustibles using FM Approved welding pads, blankets and curtains.
☐☐ Isolate potential sources of flammable gas, ignitable liquid or combustible dust/lint (e.g., shut down equipment).
☐☐ Remove ignitable liquid, combustible dust/lint and combustible residues.
☐☐ Shut down ventilation and conveying systems.
☐☐ Remove combustibles and consider a second fire watch on opposite side of floor, wall, ceiling or roof when openings exist or thermally conductive materials pass through.
☐☐ Is work on a combustible roof? If yes, treat as a "Hot Work High-Risk Area" and provide **ADDITIONAL REQUIRED PRECAUTIONS** below.

Hot work on/in closed equipment, ductwork and piping

☐☐ Isolate equipment from service.
☐☐ Remove ignitable liquid and purge flammable gas/vapor.
☐☐ Prior to work, and/or during work, monitor for flammable gas/vapor. LEL reading(s): _____
☐☐ Remove combustible dust/lint or other combustible materials.
☐☐ Is work on/in equipment with nonremovable combustible linings or parts? If yes, treat as a "Hot Work High-Risk Area" and provide **ADDITIONAL REQUIRED PRECAUTIONS** below.

Fire watch/fire monitoring the hot work area

(Refer to FM Global Property Loss Prevention Data Sheet 10-3, *Hot Work Management*, for guidance on categorizing hot work areas.)

☐ Perform a continuous fire watch during hot work.
☐ Perform a continuous fire watch following hot work completion for ☐30 or ☐60 minutes depending on category.
☐☐ Perform fire monitoring following fire watch completion for ☐1 ☐2 ☐3 ☐4 or ☐5 hours depending on category.

ADDITIONAL REQUIRED PRECAUTIONS: _____

Figure 7: Hot work permit (back view)

WARNING

HOT WORK IN PROGRESS!
Watch for fire!

In case of emergency, call the contacts listed below before attempting to extinguish the fire.

Contact	Number

Construction and Occupancy Factors for Post-Work Fire Watch and Monitoring Periods

		Construction Factors					
		Noncombustible construction, or FM Approved Class 1 or Class A building materials		Combustible construction without concealed cavities		Combustible construction with unprotected concealed cavities	
		Watch	**Monitor**	**Watch**	**Monitor**	**Watch**	**Monitor**
Occupancy Factors	Noncombustible with any combustibles contained within closed equipment (e.g., ignitable liquid within piping)	30 minutes	0 hours	1 hour	3 hours	1 hour	5 hours
	Office, retail or manufacturing with limited combustible loading	1 hour	1 hour	1 hour	3 hours	1 hour	5 hours
	Manufacturing with moderate to significant combustible loading except as noted below	1 hour	2 hours	1 hour	3 hours	1 hour	5 hours
	Warehousing	1 hour	2 hours	1 hour	3 hours	1 hour	5 hours
	Exceptions: Occupancies with processing or having bulk storage of combustible materials capable of supporting slow-growing fires (e.g., paper, pulp, textile fibers, wood, bark, grain, coal or charcoal)	1 hour	3 hours	1 hour	3 hours	1 hour	5 hours

When performing torch-applied roofing, apply additional precautions and conduct a minimum 2 hours fire watch and 2 hours fire monitoring. If an infrared camera is utilized, reduce to a 1 hour fire watch and 1 hour fire monitoring.

When performing hot work on/in equipment containing nonremovable combustible linings or parts, apply additional precautions and conduct a minimum 1 hour fire watch and 3 hours fire monitoring within the equipment, and in the surrounding areas per Table above.

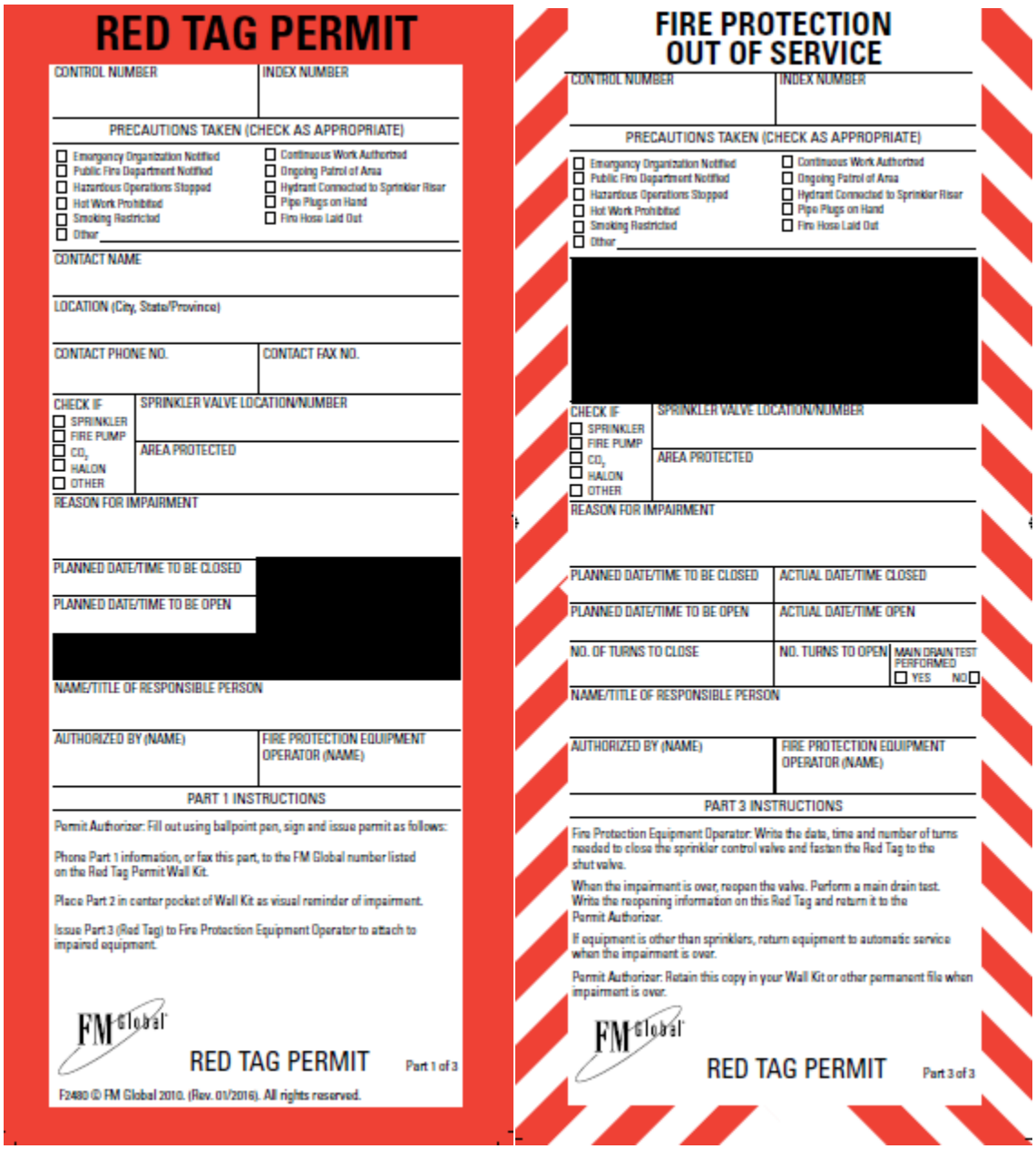
FM Global

Figure 8: Hot work permit (Page 3)

Appendix C: Impairment Form

Red Tag Permits and wall kits can be ordered through the FM Global Resource Catalog at http://www.fmglobalcatalog.com or toll free at 1-877-364-6726.

The eRed Tag permit can be access at www.fmglobal.com/redetag



RED TAG PERMIT

CONTROL NUMBER | INDEX NUMBER

PRECAUTIONS TAKEN (CHECK AS APPROPRIATE)

- ☐ Emergency Organization Notified
- ☐ Public Fire Department Notified
- ☐ Hazardous Operations Stopped
- ☐ Hot Work Prohibited
- ☐ Smoking Restricted
- ☐ Other
- ☐ Continuous Work Authorized
- ☐ Ongoing Patrol of Area
- ☐ Hydrant Connected to Sprinkler Riser
- ☐ Pipe Plugs on Hand
- ☐ Fire Hose Laid Out

CONTACT NAME

LOCATION (City, State/Province)

CONTACT PHONE NO. | CONTACT FAX NO.

CHECK IF: ☐ SPRINKLER ☐ FIRE PUMP ☐ CO_2 ☐ HALON ☐ OTHER

SPRINKLER VALVE LOCATION/NUMBER

AREA PROTECTED

REASON FOR IMPAIRMENT

PLANNED DATE/TIME TO BE CLOSED

PLANNED DATE/TIME TO BE OPEN

[redacted]

NAME/TITLE OF RESPONSIBLE PERSON

AUTHORIZED BY (NAME) | FIRE PROTECTION EQUIPMENT OPERATOR (NAME)

PART 1 INSTRUCTIONS

Permit Authorizer: Fill out using ballpoint pen, sign and issue permit as follows:

Phone Part 1 information, or fax this part, to the FM Global number listed on the Red Tag Permit Wall Kit.

Place Part 2 in center pocket of Wall Kit as visual reminder of impairment.

Issue Part 3 (Red Tag) to Fire Protection Equipment Operator to attach to impaired equipment.

FM Global

RED TAG PERMIT Part 1 of 3

FIRE PROTECTION OUT OF SERVICE

CONTROL NUMBER | INDEX NUMBER

PRECAUTIONS TAKEN (CHECK AS APPROPRIATE)

- ☐ Emergency Organization Notified
- ☐ Public Fire Department Notified
- ☐ Hazardous Operations Stopped
- ☐ Hot Work Prohibited
- ☐ Smoking Restricted
- ☐ Other
- ☐ Continuous Work Authorized
- ☐ Ongoing Patrol of Area
- ☐ Hydrant Connected to Sprinkler Riser
- ☐ Pipe Plugs on Hand
- ☐ Fire Hose Laid Out

[redacted]

CHECK IF: ☐ SPRINKLER ☐ FIRE PUMP ☐ CO_2 ☐ HALON ☐ OTHER

SPRINKLER VALVE LOCATION/NUMBER

AREA PROTECTED

REASON FOR IMPAIRMENT

PLANNED DATE/TIME TO BE CLOSED | ACTUAL DATE/TIME CLOSED

PLANNED DATE/TIME TO BE OPEN | ACTUAL DATE/TIME OPEN

NO. OF TURNS TO CLOSE | NO. TURNS TO OPEN | MAIN DRAIN TEST PERFORMED ☐ YES ☐ NO

NAME/TITLE OF RESPONSIBLE PERSON

AUTHORIZED BY (NAME) | FIRE PROTECTION EQUIPMENT OPERATOR (NAME)

PART 3 INSTRUCTIONS

Fire Protection Equipment Operator: Write the date, time and number of turns needed to close the sprinkler control valve and fasten the Red Tag to the shut valve.

When the impairment is over, reopen the valve. Perform a main drain test. Write the reopening information on this Red Tag and return it to the Permit Authorizer.

If equipment is other than sprinklers, return equipment to automatic service when the impairment is over.

Permit Authorizer: Retain this copy in your Wall Kit or other permanent file when impairment is over.

FM Global

RED TAG PERMIT Part 3 of 3

Figure 9: Red tag permit (first and last pages)

The Red Tag Permit

The fire safety supervisor uses this three-part permit to authorize the impairment and record critical information needed to manage the impairment.

Part 1:

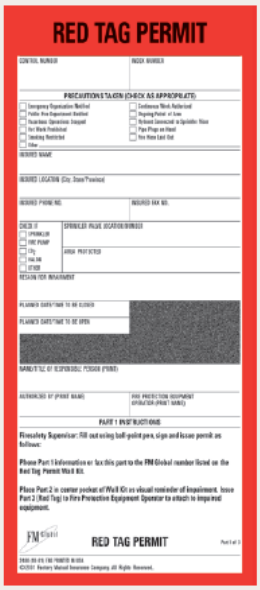
The fire safety supervisor completes the permit, signs and issues it, notifies FM Global, and follows the precautions listed.

Part 2:

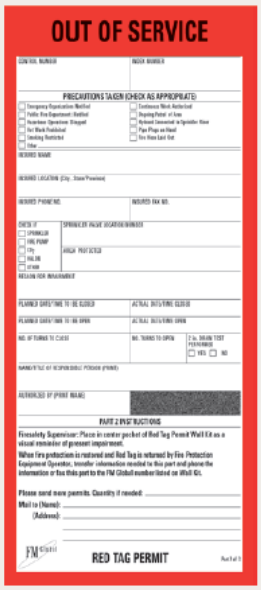
The fire safety supervisor places the permit in the center pocket of the wall hanger as a visual reminder that a valve is shut.

Part 3:

The fire safety supervisor issues the permit to the fire protection equipment operator, who documents each step of the impairment. Include date, time, type of valve and number of turns needed to close the valve. Attach the tag to the shut valve as a weather-resistant, visual reminder that a particular valve is closed. Also, attach the *Reusable Impairment Tag for Fire Service Connections* (P7427t) to the fire-service-pumper connection associated with the impaired fire protection system.



Part 1



Part 2

Part 3

Figure 10: Red tag permit (instructions)