Loss Prevention Standards – Cross Classes

Rioting/Civil Unrest

Version: 1.0
Date: 07th August 2024

Civil unrest and rioting incidents can be well-organised events with criminal elements infiltrating protest groups, or countering otherwise peaceful protests with violence and threats to persons and property.

This Loss Prevention Standard provides general guidance on reducing the risks of injury to staff, customers, and damage to property caused by rioting and civil unrest.

AVIVA

Rioting/Civil Unrest

Introduction

The number and extent of organised riots and civil unrest seen, and the associated images of violence, fire raising and looting are both shocking and concerning for the general public including employers, property and business owners who will be rightly worried about the safety of employees, guests, visitors, and customers; loss or damage to business premises, closures for repairs, threats of further rioting/unrest, and the likely costs of installing additional security measures.

It's vitally important that employers, businesses and property owners review fire, safety, and security procedures to make sure people and premises are adequately protected during periods of unrest and this Loss Prevention Standard provides guidance and simple recommendations for employers, business, and property owners, which can be implemented promptly, without incurring huge cost, and which can help reduce the potential for injury, loss, or damage.

Threats to Employees and Other Persons

Review risk assessment arrangements to make sure the control measures in place, to protect employees and others from the consequences of riot or civil unrest, are suitable and sufficient. Protection to employees and building occupants should be prioritised. Where possible:

- Prepare lockdown, evacuation, and emergency procedures, which are to be implemented in the event of unrest developing, or reports of planned unrest being issued by trusted sources.
    - Ensure all employees are aware and trained in these procedures, and where appropriate brief other building occupants.
    - Test/exercise these procedures to eliminate any areas of confusion and ensure they will work smoothly when required.
- Check news and social media updates for road closures and transport problems.
- Contact local police authorities for guidance and support.
- Ensure managers are vigilant and authorised to react quickly – there may be a necessity to close the business early to allow individuals to get home safely.
- Ensure all employees know how to raise an emerging situation or emergency event, with the public authorities e.g. who will be responsible for contacting the police?
- For whatever reason, any persons who feel particularly vulnerable should be allowed to work remotely, leave early, or stay at home if they have any concerns.
- If and where possible, temporarily relocate or adopt a homeworking policy.
- Prevent employees visiting or travelling through potential problem areas on business related activities or their commute to and from work.
- Create safe areas within the premises for individuals should they feel threatened.
- Check employees contact and next of kin information is up to date.
- Avoid unaccompanied working and issue personal alarms where appropriate.
- Make use of mobile phones and two-way radio links to maintain contact between employees across the premises.
- Firefighting equipment – ensure adequate equipment is readily available to hand and employees are trained in its use.

Employees Working Remotely

Lone working and dynamic risk assessment arrangements should be reviewed due to heightened risk levels, particularly as situations can be fast moving and change quickly. As part of any crisis management planning, all employees should be contactable straight away and provide up to date advice which may include abandoning journeys/visits and returning home. A text alert system could be used for this.

- All visits should be planned in advance.
    - News and trusted social media outlets should be monitored for any information which may impact the visit.
- Ensure mobile phones are fully charged at all times.
- Employees should be advised not to put themselves at any risk. If they don’t feel safe, then they should be told to rearrange the visit for another time.
- Managers should be aware of the location of field-based employees at all times.
- Employees should be advised to check routes before setting off. An alternative route should be planned in case the original route is blocked or disrupted.
- Employees should be advised to always park in a well-lit street, as near to the premises they are visiting, and ensuring nothing is left obvious in the car – clear front and rear seats.
- Consideration should be given as to whether wearing company branded clothing puts the employee at greater risk. If necessary, relax the rules around branded clothing.
- Make sure on route employees remain situational aware and check the surrounding areas for signs of protest, or crowds gathering.
- Prior to carrying out the visit, employees should check-in to advise they are on site and the expected duration of the visit, providing an update if the visit is extended.
- When the visit is completed, a further check-in should be carried out confirming that the visit has been completed and confirming the employee is leaving site.

Physical Damage

Intruder alarms / Video Surveillance Systems. Ensure:

- All security systems are functioning and set in their entirety whenever the premises are unattended.
- All electronic perimeter security systems are functioning and set.
- An up-to-date list of keyholders is held by relevant stakeholders and authorities, including your Alarm Receiving Centre(s).

Physical security to buildings.

- Ensure any fencing is in good repair and gates are locked/secured.
- Ensure existing perimeter barriers are in good repair; doors and door hardware are adequate and in good repair; and accessible windows are adequately secured and protected.
- Grilles/shutters should be maintained in position throughout all hours (even during opening hours).
- Consider temporary, external boarding of vulnerable access points and windows particularly in high-risk areas. Alternatively glazing security films can hold damaging glass in position, providing some resistance to attack.
- Discuss jointly funded security guarding services with neighbouring businesses. This can provide enhanced security protection at a shared cost.
- Leave internal lighting off overnight and maintain external lighting, if and where possible, or configure security lighting so it is operational throughout all hours of darkness, where safe to do so (continual use of high-powered lighting may create an increased fire risk)
- Check automatic fire alarm systems are fully functioning.

- Remove lightweight objects such as waste bins, advertising hoarding etc., which may be used to damage buildings and glazing.
- Waste and other unwanted combustible materials are an obvious source of ignition and may be targeted, and hence should be either removed from site or kept to a minimum and adequately secured.
- Cut back any vegetation in proximity to the premises.
- Isolate any utilities such as gas, water supplies and unnecessary electric circuits, where safe to do so, if a threat of rioting/civil unrest in the locality has been reported by a trusted source.

In respect of cash, high value contents and stock:

- Remove cash and empty ATM's where possible.
- Remove high value, or theft attractive stock to safe storage elsewhere. Where this isn't possible, move high value, or theft-attractive stock to a physically robust and secured room or compound.
- Remove attractive stock from display windows.
- Consider delaying the delivery of theft attractive stock until the immediate threat of rioting and unrest has subsided.

To help avoid the potential for damage to vehicles in the open:

- Remove and avoid parking vehicles overnight in high-risk areas and on main thoroughfares
- Avoid parking vehicles in close proximity to buildings
- Garage Forecourts – avoid storage/display of vehicles on forecourts in high risk areas in the short term, preferably to a secure compound wherever possible
- Physical Guarding – consider introduction of security guards increasing the hours of guarding presence and/or increasing the number of guards present

Business Continuity

Business Continuity Plans should be reviewed to ensure disaster recovery and continuity arrangements remain adequate. Any actions generated should be addressed promptly.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

- VSS and detection security: Secom.
- Forensic/DNA marking: Selectamark.
- Vacant Property, Site Security and Lone Working Services: Orbis.
- Fire alarms: Secom Fire
- Business resilience: Horizonscan.

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Additional Information

Relevant Loss Prevention Standards include:

- Security - Locks.
- Security - Intruder Alarms - Guidance for Customers.
- Arson Prevention.
- Lone Working.
- Violence to Employees.
- Business Continuity.

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential, or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

7th August 2024

Version 1.0

ARMSGI1912024

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.