# **Developing security alert levels: A good practice guide**

Use this guide to help you develop the alert levels your organisation needs to move to heightened security in case of emergency or increased threat.

The advice in this guide applies to:

* people working in security management
* contractors who provide security advice and services to government agencies
* anyone who is responsible for the security of New Zealand people, information, or assets.

# How this guide fits with government requirements

This guide supports the implementation of the Protective Security Requirements (PSR). Under the PSR, government agencies must develop plans and be ready to move to heightened security levels when necessary.

|  |
| --- |
| **GOV 7 – Be able to respond to increased threat levels**  Develop plans and be prepared to implement heightened security levels in emergencies or situations where there is an increased threat to your people, information, or assets. |

The following requirements are related to security alert levels:

* Developing protective security policies, plans, and processes
* Management protocol for physical security
* Management protocol for information security
* Business Impact Levels.

Base your decisions about security alert levels on whichever requirements are the highest —the advice in this guide, the related requirements listed above, or any legislation that applies.

# Why you need to develop security alert levels

Security alert levels communicate information about the security measures you use to reduce risks in emergency situations and other times of heightened risk.

Alert levels also allow you to scale the security measures you use, so they’re appropriate to the type of incident and can change easily as risks increase or decrease.

Developing alert levels helps your organisation to apply security measures quickly before or during an incident. A quick response can greatly increase your ability to protect your people, information, and assets.

# How to develop security alert levels

Take an ‘all hazards’ approach to developing alert levels. That means including all types of threats from all sources, so you can generate a balanced response. Physical and environmental threats may have the same, or greater, impact on your organisation’s ability to function as traditional security threats.

Any protective security measures you implement with your alert levels should mitigate the risks to your people, information, and assets. They should also make any information and asset sharing arrangements you have more secure.

## Work out your sources of physical risks

Base your alert levels on possible sources of risk to your security — risks you’ve identified in your organisation’s security risk assessment.

Sources of physical security risks fall into three main categories:

* **Event** – an important happening or incident that affects your organisation’s ability to function. Examples include a weather event such as a storm or an emergency event, such as an earthquake.
* **Threat** – a declared intent and capability to inflict harm on your people, information or property.
* **Activity** – an action by one or more people likely to have a negative impact on physical security. For example, protest activity, occupation or attempted occupation, or filming near your premises.

If your protective security measures are damaged or breached by an event or activity, or you have reliable evidence to support the possibility of a threat, then you may need to escalate the alert level.

## Assess the unique risks of each facility or work area

Each facility or work area within a facility may have unique security risks. To identify and assess the physical security risks likely to affect each site during events, threats, or activities, your security management people should work with:

* local managers responsible for each facility
* people involved with business continuity, disaster recovery, and risk management.

## Draw on internal and external sources of information

Seek information on risks from internal and external sources.

### Internal sources

Your organisation’s overall risk assessment is an excellent source of information. Check the assessment and consult with your business areas to learn more.

Your business areas should be able to tell you about:

* the business impact of disruptions to their operations, harm to their people, or the compromise or loss of information or assets
* when Business Impact Levels (BILs) may change due to changes in an asset’s importance (for example at the end of a project).

Other important internal sources of information about risks are your:

* protective security risk reviews
* security incident and staff reports
* security and operational risk registers.

### External sources

External sources include any organisations you work, partner, or co locate with. You should consider the BILs of any collaborative work or sharing arrangements. Do the other agencies have unique risk factors and how might they affect your combined business continuity plans?

Other examples of external sources of information you can draw on are:

* the national alert level
* national threat assessment advice
* Police, MetService, and Civil Defence advisories
* National Cyber Security Centre (NZSC) and CERT NZ
* media reports.

## Take care not to under- or over-protect

When you’re designing or selecting alert levels, aim for a balanced approach as over- or under-protecting your people, information, and assets can create problems.

### Over-protection

Over-protection is costly, inefficient, and can be an obstacle to your operations. Over-protection is often caused by:

* personal interpretation of the level of harm possible from a risk source
* not having enough alert levels to allow staged escalation of measures appropriate to the increase in risk.

### Under-protection

Under-protection can affect personal safety, and the security of your information and assets.

To prevent under-protection, provide guidance that makes it easy for your people to identify which risk sources require an increase in alert level. And make that increase easy to implement.

## Decide how many alert levels you need

The number of alert levels to use depends on your operating environment and expected changes in your risk sources. Essential factors to consider are the nature of your organisation, the types of facilities you use, your operational role, and known risk levels.

### Examples of alert levels

The following four examples of alert levels show how you can**:**

* define an alert level
* describe the situations each level covers
* summarise the measures that apply to each level.

#### Low

This security alert level applies when there is little likelihood of an event causing harm. The security measures in place would meet normal internal operational requirements.

|  |  |  |
| --- | --- | --- |
| LOW ALERT LEVEL  Applies when only general concerns exist or no known event, general threat, or physical activity likely to cause harm to the organisation or any of its facilities exists.  Measures can be maintained indefinitely. | | |
| **Example event, threat, or activity** | | **Measures** |
|  | **Event**   * MetService and GeoNet routinely checked – no environmental impacts are considered likely. | * Staff are reminded about security and alert issues. * Operational security and emergency plans and procedures are reviewed (at least once per year). * Awareness training activities are initiated. |
|  | **Threat**   * A terrorist attack is assessed as unlikely. |
|  | **Activity**   * General concerns around criminal activity such as vandalism or theft exist, but no significant impact to business and staff is expected. |

#### Medium

This security alert level applies when an event, general threat, or physical activity likely to cause harm might occur. However, there is no specific threat directed to your organisation or facilities.

Any security measures you apply can be maintained indefinitely, with minimal impact to your organisation’s operations.

|  |  |  |
| --- | --- | --- |
| MEDIUM ALERT LEVEL  Applies when an event, general threat, or physical activity likely to cause harm might occur. There is no specific threat directed at the organisation or any of its facilities.  Measures applied can be maintained indefinitely. | | |
| **Example event, threat, or activity** | | **Measures** |
|  | **Event**   * A general storm or tsunami warning is issued by the MetService for the general area. | * Staff are alert to unusual activities and know who to report them to. * Normal operational plans and procedures are up to date. * Regular security and emergency awareness messages are issued. * Staff and emergency control personnel are trained and alert to local emergency events. * Security, threat, and disaster recovery plans are reviewed annually. |
|  | **Threat**   * A terrorist attack is assessed as feasible and could well occur, but no specific threat is known. |
|  | **Activity**   * An unannounced protest activity (by groups or an individual) could occur near or against the organisation’s premises. |

#### High

This security alert level applies when an event, threat, or physical activity likely to cause harm is expected to occur to your organisation or any of your facilities.

Any security measures you apply can be maintained for lengthy periods without causing undue hardship to your people, affecting operational capability, or aggravating relationships with the local community.

|  |  |  |
| --- | --- | --- |
| HIGH ALERT LEVEL  Applies when an event, threat, or physical activity expected to cause harm is likely to occur to the organisation or its facilities.  Measures can be maintained for lengthy periods without causing undue hardship, affecting operational capability, or aggravating relations with the local community. | | |
| **Example event, threat, or activity** | | **Measures** |
|  | **Event**   * An extreme weather event or tsunami warning is issued by the MetService for the area. * A fire alarm has been activated for an unknown reason. | * Low to medium security measures are in place. * Warning lights may be in operation for limited periods. * Emergency control personnel are alerted and emergency procedures deployed where required. * Staff are notified of the change in alert level. * Additional screening procedures and/or visitor restrictions are in place. Restrictions may include no visitors allowed, and vehicles being subject to inspections or limited access. * Alternative business operation strategies are considered when an assessment of the situation finds the measures must be maintained. |
|  | **Threat**   * An assessment exists that a terrorist attack is feasible and could well occur to the organisation. * A suspicious mail item is received in the mail. |
|  | **Activity**   * A known protest activity (by groups or an individual) is to occur near or against the organisation’s premises, but no acts of violence are anticipated. |

#### Extreme

This security alert level applies when an event, threat, or physical activity likely to cause significant harm is imminent or has occurred to your organisation or any of your facilities.

You won’t be able to maintain the necessary security measures for lengthy periods and they may cause hardship to your people, affect operational capability, or aggravate relationships with the local community.

|  |  |  |
| --- | --- | --- |
| EXTREME ALERT LEVEL  Applies when an event, threat, or physical activity likely to cause significant harm is imminent or has occurred to the agency or its facilities.  Measures will create hardship, affect the activities and personnel in the location, are not sustainable over the long term, and may have implications for other premises depending on the type of incident. | | |
| **Example event, threat, or activity** | | **Measures** |
|  | **Event**   * An extreme weather event or tsunami is occurring or has occurred that is directly impacting on the organisation and staff. * A significant earthquake has occurred that is directly impacting on the organisation and staff. * A fire alarm has been activated for a fire or emergency event and involves the evacuation of staff. | * Low, medium, and high security measures are in place. * Premises and surrounding areas are locked down. * No visitors are allowed, and vehicles are subject to inspections and limited access. * Mail and other deliveries are suspended. * Critical, security, and emergency control staff are on alert or deployed. * Frequent communication with staff. * Plans are under constant review until alert is returned to HIGH. |
|  | **Threat**   * An assessment exists that a terrorist attack is imminent and could well occur or has occurred to the organisation. * The organisation receives a bomb threat. |
|  | **Activity**   * Protest activities (by groups or an individual) are occurring near or against the organisation’s premises, and acts of violence are anticipated or underway. |

#### More alert level examples

The ‘National alert levels table’ (Annex A on page 12)shows alert levels for risks associated with terrorism and violent criminal behaviour. However, these alert levels may not be suitable for all organisations and do not reflect all of the hazards your organisation might face.

## Work out and confirm your security measures

Use your assessment of risk sources and operational requirements for each facility to work out which security measures you need for each alert level.

Several generic measures might be suitable at each alert level. For examples, see ‘Annex B:Operational security measures for alert levels’ on page 13**.**

Your security management people should work with local area managers and consult with your risk managers to develop procedures for each facility and risk source.

**Monitor your risk environment and change when necessary**

You should actively monitor your organisation’s risk environment and change (increase or decrease) the alert level to match any changes to the risks.

## Develop a guide to your security alert levels

Developing a guide will help you refine your alert levels and associated security measures. It’s important to consult the different business areas in your organisation. Aim to find out if your guide will be effective or have implications for other security processes within your organisation.

Once your guide is developed, it will be a vital source of information about your security alert levels.



Figure 1 —Development process for a guide to security alert levels

## Develop a communications plan

Communicating a change in alert level well is essential to getting the right responses. Your people need to know what has changed and what to do.

Your communications plan will help you create a successful strategy. You need to consider the audiences, messages, methods, and responsibilities.

**Audiences**: Who needs to know about the alert and what do they need to know? Different communication may be required for different audiences (senior management, staff, security staff).

**Messages**: Which messages do you need to communicate to each audience? Aim to create concise and unambiguous statements that clearly identify the issues and the actions required.

**Methods:** How will you communicate the messages? Choose the best medium or combination of mediums to get your messages to your audiences as quickly and effectively as possible.

**Responsibilities**: Your strategy should clearly identify:

* who is responsible for determining the alert level (this may differ for each level and facility)
* any specific roles or responsibilities for other positions, as well as all staff.

Ask your communications team for expert advice when you’re developing the communications plan.

### Related guidance

HB167:2006 Security risk management [add link]

This handbook suggests using the IRACI tool (Intervention, Responsibility, Accountability, Consult and Inform) to work out who needs to be involved in developing the strategy.

## Review and update your processes

You should review your alert level processes:

* when you take on new projects
* as the risk environment changes
* after a significant incident that affects your ability to operate
* at least every 2 years.

Practise and review the activation procedures for your alert levels as well as the security measures for each level. Use what you learn to identify any gaps and update your guide.

### Debrief after going to high or extreme alert levels

A debrief can be helpful for improving your response. Consider debriefing after every alert level change to ‘high’ or ‘extreme’. A debrief should consider:

* why the alert level change was initiated
* how the alert level change was initiated
* what activity and actions were undertaken for the alert level change
* what and where, if any, improvements could be made to alert level procedures and communications.

**Annex A: National threat level table**

|  |  |  |
| --- | --- | --- |
| **Threat level** | **Definition** | **Qualitative statement** |
| Negligible | Terrorist attack, violent criminal behaviour, or violent protest activity is assessed as very unlikely | Remote / Highly unlikely |
| **Very low** | Terrorist attack, violent criminal behaviour, or violent protest activity is assessed as unlikely | Improbable / Unlikely |
| **Low** | Terrorist attack, violent criminal behaviour, or violent protest activity is assessed as possible, but is not expected | Realistic possibility |
| **Medium** | Terrorist attack, violent criminal behaviour, or violent protest activity is assessed as feasible and could well occur | Probable / Likely |
| **High** | Terrorist attack, violent criminal behaviour, or violent protest activity is assessed as likely | Highly / Very probable / Likely |
| **Extreme** | Terrorist attack, violent criminal behaviour, or violent protest activity is expected imminently | Almost certain |

**Annex B: Operational security measures for alert levels**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Alert level** | **Example trigger: Event, threat, or activity** | **Doors** | **Visitors** | **Contractors** | **Mail and**  **deliveries** | **Staff** | **Police** | **Guards** | **Business impact** |
| **Normal** |  | **Normal operation** | **As per visitor policy** | **As per contractor policy** | **As per policy** | **Normal awareness** | **Not required** | **Normal operation** | **Normal** |
| **Low** | **Protest**  **Threat received** | **Normal operation** | **As per visitor policy** | **As per contractor policy** | **Additional screening of all mail and deliveries** | **Security team or manager advises of potential risk by email and in person**    **Reminded to be alert to and report unusual activities** | **Not required** | **May be required at main door** | **No effect or impact on normal operations** |
| **Medium** | **Protest or demonstration expected or underway**  **Violent protest in the area**  **Non-specific bomb threat**  **Increased weather risk**  **Threat of harm to staff** | **Doors put into night mode**  **All doors require access card** | **No ‘non-essential’ visitors (effectively no visitors, but in certain circumstances a known visitor or conference may be the cause for activity)** | **No non-essential contractors**    **Only security related contractors working on maintaining security functions allowed** | **Additional screening of all mail and deliveries** | **Advised when arriving and leaving to be alert and ready to change plans at short notice if necessary** | **Police advised and may be required depending on event** | **Guard at main door**  **Permanent CCTV monitoring** | **No visitors, minimal impact on normal operations** |
| **High** | **Current threat (violent protest)**  **Natural disaster, severe weather event**  **Major internal incident, such as fire or flooding** | **Access control cards disabled on external doors**  **Guards control external doors** | **No visitors** | **No contractors** | **No unexpected mail or deliveries accepted**  **All mail deliveries checked at alternate location** | **Essential staff only**  **Non-essential staff called and advised not to come to work**  **Start preparations to transfer critical functions to alternate site at short notice** | **Police necessary** | **Search all**  **employees’ bags**  **Prevent unauthorized entry** | **Only essential business operations** |
| **Extreme** | **Out of control and violent protest or riot or terrorist event imminent or expected**    **Potential for physical harm**  **Major natural disaster** | **Doors mechanically secured and locked with keys** | **No visitors** | **No contractors** | **No contractors** | **Facility closed, and essential operations conducted at alternate site**  **Staff called and advised not to come to work**    **Nobody enters or leaves the building** | **Police necessary** | **Guards at all doors** | **Essential operations conducted at alternate venues** |