PSR | Protective Security Requirements

DEVELOPING AGENCY ALERT LEVELS

A GOOD PRACTICE GUIDE

Introduction

The Protective Security Requirements (PSR) requires agencies to have plans and protocols in place so they can move to heightened security levels in case of emergency or increased threat (PHYSEC 7). This good practice guide—provides advice to assist agencies with this process.

Mandatory requirement PHYSEC 7

Agencies must develop plans and protocols to move up to heightened security levels in case of emergency and increased threat. The New Zealand Government may direct its agencies to implement heightened security levels.

Audiences

- New Zealand government security management staff.
- Contractors providing protective security advice and services to government agencies.
- Any other body or person responsible for the security of New Zealand people, information or assets.

Scope

This guide provides best practice advice to agency staff. Specific controls and risk mitigation measures used by agencies should be based on the requirements of legislation or the PSR and supporting protocols and guidelines, whichever is the higher.

This guide supports the implementation of the Protect Security Requirements (PSR).

In particular they support:

- *physical security management protocol*
- *security Zones and risk mitigation control measures*
- *physical security of ICT equipment, systems and facilities*
- *business impact levels*.

Approach

Agencies should integrate the preparation of their alert levels with other protective security policies, plans and procedures. Also refer to: Developing agency protective security policies, plans and procedures.

Why develop an alert level system?

An alert level system is one of an agency's protective security procedures. It provides employees with information about the measures used by an agency to mitigate risks in the effect of emergency situations and or heightened threat levels. Alert levels are an easily understood and scalable method of implementing controls appropriate to the type of incident. Applying controls quickly when you are forewarned of a possible incident, or during an incident greatly increases your ability to protect your people, information, and assets.

Alert levels should take an 'all hazards' approach as physical and environmental threats may have the same, or greater, impact on an agency's ability to function as traditional security threats.

A system that follows an all hazards approach aims to include all types of threats, irrespective of origin, and generate a balanced response.

Sources of information used to determine alert levels

The source of agency physical security risks may be categorised into three areas:

- **Event** – an event is an important happening or incident impacting on the agency's ability to function. Examples include a weather event (e.g. storm) or an emergency event (e.g. earthquake).
- **Threat** – a declared intent and capability to inflict harm on agency staff or property.
- **Activity** – an activity is an action by one or more people likely to have a negative impact on physical security (e.g. protest activity, occupation or attempted occupation, filming in the vicinity of premises).

If an agency's protective security measures are damaged or breached by an event or activity, or there is reliable evidence to support a threat, then the response might necessitate an escalation of the agency alert level.

Information that may be drawn on in determining an alert level includes, but is not limited to:

- the National Alert Level
- agency protective security risk reviews
- national threat assessment advice
- local Police advice
- MetService advice
- agency security incident reports
- media reports, or
- staff incident reports.

Implementing appropriate alert levels based on risks

Protective security measures should mitigate the risks to agency personnel, information and assets as well as provide assurance in relation to information and asset sharing arrangements. Alert levels allow agencies to scale the controls used to mitigate threats as the risks increase or decrease.

Agency specific alert levels should be based on possible sources of risk to the agency's physical security identified in the agency security risk assessment. The number of alert levels an agency needs will be determined by their risk sources and operating environment.

Inappropriate design or selection of alert levels can lead to over-protection or under-protection of people, information and assets.

Over-protection

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

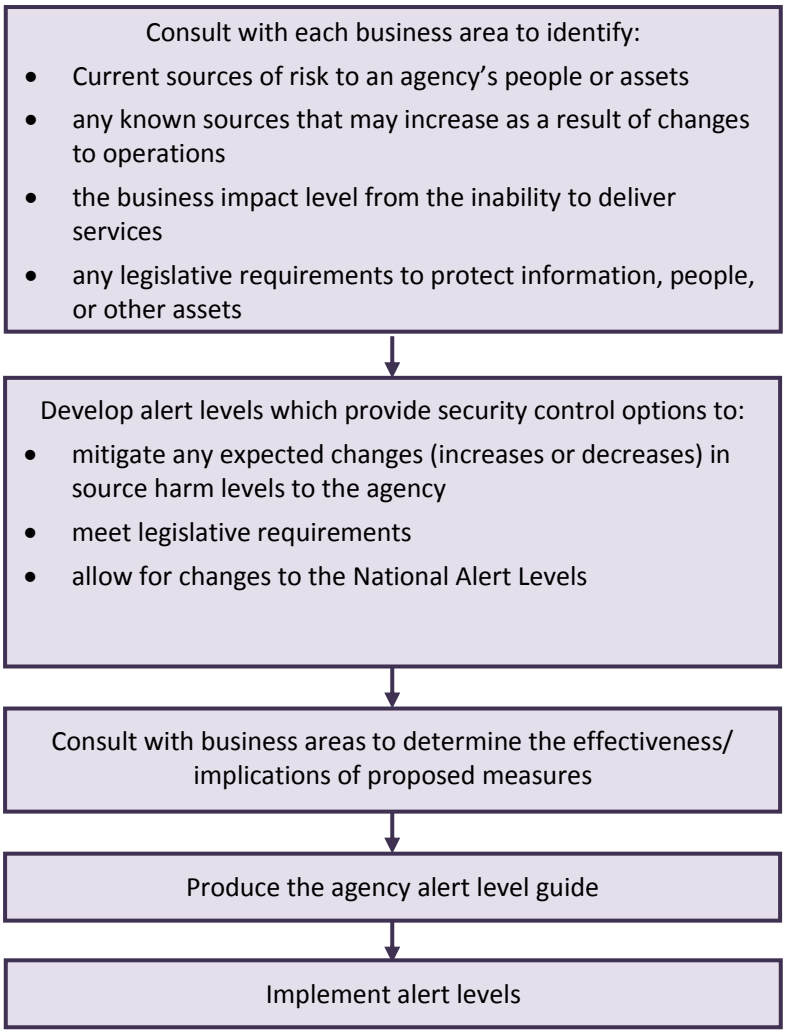
- personal interpretation of the level of harm possible from a risk source, or
- not having sufficient levels to allow staged escalation of measures appropriate to the increase in risk.

Under-protection

Under-protection can impact personal safety, as well as information and asset security. Agency alert level guides should include guidance so that risk sources requiring an increase in alert level are readily identified. The increase in alert level should also be easily implemented.

Developing an agency alert level guide

Figure 1—Alert level guide development process



Consultation

Internal agency consultation

An agency risk assessment process should include consultation to determine the criticality of agency operations and assets, including people, information and physical assets, using a business impact level assessment. This should include consultation on the agency alert level guide. Business areas should:

- know the business impact resulting from disruption to their operations, harm to their people or compromise, or loss of information or assets,
- be able to identify when the business impact level may change due to changes in the asset's importance, for example at the conclusion of a project.

See the *Business impact levels.*

Each facility within an agency may have their own unique security risks. These risks may also be different for individual work areas within a facility. Agency security management personnel should work with:

- local managers responsible for the facility,

- agency business continuity, disaster recovery and risk management personnel to identify the key physical security risks likely to impact the site in events, threats or activities.

Agencies may also use their security and operational risk registers to identify potential sources of risk and the impact of these risks.

Inter-agency and partner consultation

When an agency works with other partners, on projects or co locations, it should consider the business impact levels of the collaborative work. Consideration for other risk factors unique to the other agencies must be made, and assess how they may affect business continuity in partnership.

Number of alert levels

The number of alert levels for each agency will depend on operational requirements and expected changes in risk sources. The starting or base level for an agency or facility will depend on the type of agency/ facility, operational role and known risk levels.

The following example alert levels at **Annex A** consist of four levels:

- **Low**
  - Applies where there is little likelihood of an event causing harm to the agency or agency facilities.
  - Security measures in place meet normal internal operational requirements.
- **Medium**
  - Applies when an event, general threat, or physical activity likely to cause harm might occur. There is no specific threat directed to the agency or agency facilities.
  - Any security measures applied are maintainable indefinitely, with minimal impact to the organisations operations.
- **High**
  - Applies when an event, threat, or physical activity likely to cause harm is expected to occur to the agency or any agency facility.
  - Any security measures applied are maintainable for lengthy periods, without causing undue hardship to staff, effecting operational capability, or aggravating relationships with the local community.
- **Extreme**
  - Applies when an event, threat, or physical activity likely to cause significant harm is imminent or has occurred to the agency or agency facility.
  - Any security measures applied will not be maintainable for lengthy periods and may cause hardship to staff, affect operational capability, or aggravate relationships with the local community.

The National Alert levels table at **Annex B** is a further example of alert levels that agencies may consider adopting. The National Alert Levels may not be suitable for all agencies; each agency must determine the number of levels that will be appropriate for their organisation or facility. The National Alert Levels definitions relate to terrorism and violent criminal behaviour and do not reflect the All Hazards approach that should be considered by agencies.

Control Measures

The controls required are determined by the assessment of the risk sources and operational requirements for each facility. There are a number of generic options that may be considered in dealing with controls at each alert level, an example of Operational Alert Level Controls can be seen at **Annex C.**

Agency security management staff working with the local area managers, and in consultation with the agency risk managers, should develop procedures specific to the facility and the source.

Implementing alert levels

Agencies should actively monitor their risk environment and change (increase or decrease) the alert level to meet any changes to the risks.

Communicating information about Alert Levels

Agencies should develop a communication plan around the alert levels. The plan should consider:[1]

- **audience** – Who needs to know about the alert and what do they need to know. There may be different communication required depending on the audience (senior management, staff, security staff)
- **message** –what is the message you want to direct to your audience (a clear, concise , and unambiguous statement identifying the issue and detailing the actions required),
- **method** – or the means by which you will communicate the message. This will depend on the available technology and preferences of the recipient of the message.

The strategy should clearly identify who is responsible for determining the alert level (this may be different for each level and at each facility). The communications plan should also clearly identify any specific roles or responsibilities for other positions as well as all employees.

The assistance of the agency communications team should be sought when developing the communications plan.

Annex A contains example alert level posters.

Annex B contains the National Alert Level Table

Annex C contains an example Alert Level Operational Table

[1] See *HB167:2006 Security risk management*. The handbook suggests a tool IRACI (Intervention, Responsibility, Accountability, Consult and Inform) can help to determine who needs to be involved in developing the strategy.

Review and update of alert level procedures

Review and update of alert level procedures

Agencies should review their alert level procedures:

- when they undertake new projects
- as the risk environment changes
- after a significant incident impacting on the agency's ability to operate, or
- at least every two years.

The agency should review and practice the activation procedures for the alert levels as well as the controls used for each level. The review will enable agencies to identify any gaps in their alert levels and update their alert levels guide.

Agencies should consider undertaking a debrief after every alert level changes that involves an increase to your agencies documented alert level at the high or extreme end. The 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

Such reviews should be used to improve on the procedures around alerts.

LOW

Applies when only general concerns exist or no known event, general threat, or physical activity likely to cause harm to the agency or any of its facilities exists.

Example event, threat, or activity	Measures
 Event: ▸ MetService and Geonet routinely checked – no environmental impacts considered likely.  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 expected.	All measures applied under this alert level are to be capable of being maintained indefinitely. ▸ 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.

MEDIUM

Applies when an event, general threat, or physical activity likely to cause harm might occur. There is no specific threat directed at the agency or to any of its facilities.

Example event, threat, or activity	Measures

All measures applied under this alert level are to be capable of being maintained indefinitely.

Event:

- A general storm or Tsunami warning is issued by the MetService for the general area.

Threat:

- A terrorist attack is assessed as feasible and could well occur but no specific threat is known.

Activity:

- An unannounced protest activity could occur against the agency's premises by groups or an individual.

- Staff are alert to unusual activities and 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.
- Annual review of security, threat and disaster recovery plans.

HIGH

Applies when an event, threat, or physical activity expected to cause harm is likely to occur to the agency or its facilities.

Example event, threat, or activity	Measures

The measures used under this alert are to be capable of being maintained for lengthy periods without causing undue hardship, affecting operational capability, or aggravating relations with the local community.

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.

Threat:

- An assessment exists that a terrorist attack is feasible and could well occur to the agency; a suspicious mail item is received in the mail.

Activity:

- A known protest activity is to occur near or against the agency's premises by groups or an individual but no acts of violence are anticipated.

- LOW/ MEDIUM 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 are in place and/or visitor restrictions including possibility no visitors are allowed and vehicles subject to inspections or limited access.
- Alternative business operation strategies are considered where an assessment of the situation finds the measures are to be maintained for lengthy periods of time.

Extreme

Applies when an event, threat, or physical activity likely to cause significant harm is imminent or has occurred to the agency or its facilities.

Example event, threat, or activity **Measures**

The measures used under this alert will create hardship and affect the activities and personnel in the location. These conditions are unlikely to be sustainable over the long term without having an impact on business.

Normally, this condition will be declared as a localised response but it may have implications for other agency premises depending upon the type of incident.

Event:

- An extreme weather event or Tsunami is occurring or has occurred that is directly impacting on the agency and staff; a fire alarm has been activated for a fire or emergency event and involves the evacuation of staff.

Threat:

- An assessment exists that a terrorist attack is imminent and could well occur to the agency or has occurred.
- The agency receives a bomb threat.

Activity:

- Protest activities are occurring near or against the agencies premises by groups or an individual and acts of violence are anticipated or underway.

- LOW/ MEDIUM and HIGH 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 delivery suspended.
- Critical, security and emergency control staff on alert or deployed.
- Frequent communication with staff.
- Plans under constant review to returning alert to HIGH or LOW/ MEDIUM level.

National Threat level Table **Annex B**

Threat level	Definition	Qualitative Statement
Negligible	Terrorist attack, or violent criminal behaviour, or violent protest activity is assessed as very unlikely	Remote / Highly Unlikely
Very Low	Terrorist attack, or violent criminal behaviour, or violent protest activity is assessed as unlikely.	Improbable / Unlikely
Low	Terrorist attack, or violent criminal behaviour, or violent protest activity is assessed as possible, but is not expected.	Realistic Possibility
Medium	Terrorist attack, or violent criminal behaviour, or violent protest activity is assessed as feasible and could well occur.	Probable / Likely
High	Terrorist attack, or violent criminal behaviour, or violent protest activity is assessed as likely.	Highly / Very Probable / Likely
Extreme	Terrorist attack, or violent criminal behaviour, or violent protest activity is expected imminently.	Almost Certain

Alert Levels Operational Table (Example only)

Annex C

Alert Level	Example Trigger Event, Threat, or Activity	Doors	Visitors	Contractors	Mail/ 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	• Advised of potential risk by email and verbally by Security team or manager • Reminded to be alert to and report unusual activities.	Not required	Guards may be required at main door	no effect or impact to normal operation
Medium	• expected/currently a protest or demonstration • 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 in order to maintain security functions.	Additional Screening of all mail and deliveries	• Staff advised to be alert and ready to change plans at short notice if necessary when coming/leaving.	Police advised may be required depending on event	Guard at main door Permanent CCTV monitoring.	no visitors, minimal impact to normal operation
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	Bag search Employees' Prevent unauthorized entry	only essential business operation
Critical	• Out of control Violent protest/riot/terrorist event imminent or expected, • Potential for physical harm. • Major natural disaster.	Doors mechanically secured/key locked.	No visitors	No contractors	No contractors	• Facility closed and essential operations conducted at alternate site. • Staff called advised not to come to work. • Nobody enters or leaves the building.	Police necessary	Guards at all doors	Essential operations conducted at alternate venues.