Proactively released by New Zealand Police

Operation security

This document was current as at 30 May 2022. Police policies are regularly reviewed and updated.
The most current version of Police policies are available from www.police.govt.nz

Proactively released by New Zealand Police

Table of Contents

This document was current as at 30 May 2022. Police policies are regularly reviewed and updated.
The most current version of Police policies are available from www.police.govt.nz

Proactively released by New Zealand Police

Executive summary

OPSEC is the process of protecting individual pieces of data or information which, if grouped together, could inadvertently divulge operational plans, techniques or teams. OPSEC involves protecting information deemed mission critical by operations commanders, senior leaders, management or other decision-making bodies.

The OPSEC process leads to development of countermeasures which include technical and non technical measures which protect Police tactics techniques and procedures

There is a clear distinction between security on operations and OPSEC. OPSEC is “the process which gives a Police operation or exercise appropriate security, using passive or active means, to deny subject(s) or suspect(s) knowledge of the dispositions, capabilities and intentions of the Police.”

Key critical points

Police must be aware of these key, critical points of OPSEC:

Health and safety: The overriding principle of OPSEC health and safety is to apply TENR ensuring that 'safety is success'. Victim, public and employee safety are paramount, and every effort must be made to minimise harm and maximise safety.

-

Surprise: Surprise cannot be achieved without good security The success of operations depends in great measure on the element of surprise and on the steps taken to prevent knowledge of Police intentions reaching our subject(s) or suspect(s)

-

Security: Security enhances freedom of action by limiting knowledge of our vulnerabilities to the target of our activities and threats. The main objective is to prevent the subject(s) or suspect(s) obtaining information about our intentions, operation orders, vulnerabilities, deployment and movements, which would allow them to avoid our operation.

Note: Well-planned OPSEC measures will enhance an operation and its effectiveness, not constrain it.

Proactively released by New Zealand Police

Overview

Use by operation commanders

Operations commanders use OPSEC to protect a planned operation from harm or compromise. Effective OPSEC ensures essential secrecy and surprise while stopping a subject(s) or suspect(s) from developing and implementing countermeasures to Police operational intentions and capabilities.

Responsibilities

When planning and conducting any sensitive exercise or operation, all managers must consider what possible detrimental impact any inherent OPSEC vulnerability can have on the effectiveness of that exercise or operation. Apply the need-to-know principle.

Operation commanders must critically examine sensitive activities, which, if they were disclosed, could potentially compromise their execution, or introduce reputational risks.

Note: Security remains a command responsibility during operations.

Definitions

This table defines terms relevant to operation security.

Term	Definition
	s.6(a) OIA

Proactively released by New Zealand Police

s.6(a) OIA

Proactively released by New Zealand Police

OPSEC indicators and process

OPSEC indicators

Some Police activities involve a regulated or predictable sequence or pattern of events; some planned and some unplanned. These regular sequences and patterns may be present during the planning, preparation, or execution stages of an activity. They can create vulnerabilities that may be observed by subject(s)/suspect(s) or other entities, either sympathetic to them, or in opposition to Police activity and subsequently exploited.

Through the analysis of actions and data relating to the stages of an activity, it can be determined how a subject(s) or suspect(s) could obtain critical information regarding Police operations, even if completely denied access to all classified and sensitive aspects of the activity by effective security measures.

Detectable activities and related data that can be pieced together like a jigsaw to derive a clearer view of activities are called indicators. Typically, the indicators are unclassified, and often beyond the purview of traditional protective security programmes. Usually, indicators most easily accessible to an adversary occur in support activities such as administration, travel, budgeting, engineering maintenance and acquisitions. The effect of aggregation of the indicators may change the value of the data to require a higher security classification.

OPSEC process

The OPSEC process has these five stages.

Stage	Description
1 **Identification of critical information**	This stage involves determining what information imparted in the planning or execution of a particular activity, if known by a subject(s) or suspect(s), could be used to cause damage to the effectiveness of that activity. That information is what all subsequent steps in the OPSEC process are devised to protect. **Note**: Critical information may change at different phases of an operation.
2 **Identification and analysis of the threat**	The purpose of this stage is to identify as precisely as possible the subject(s) or suspect(s) from whom the critical information must be denied. Subsequently, it involves the assessment of their capabilities, the intent and their opportunity to collect, analyse and detrimentally use the information obtained.
3 **Identification and analysis of the vulnerabilities**	This stage seeks out potentially damaging indicators of critical information through detailed analysis of how the activity is being (or is planned to be) conducted The chronology of all events timings of actions flow of information and materials and movement of people are all examined for observable actions or data that could be interpreted or pieced together to yield underlying critical information **Note:** Indicators may change during different phases of an operation.
4 **Assessment of the risks**	Following the identification of the threats and vulnerabilities this stage matches information gathered to provide a basis to assist a determination of whether any countermeasures are required Assigns a risk level derived from a consideration of the threat associated with each vulnerability This is the unmitigated risk level prior to the application of countermeasures
5 **Application of appropriate countermeasures**	This concluding stage is determining the extent and application of any appropriate countermeasure. Such countermeasures may include procedural changes to an activity or plan, cover and deception, enhancement of existing protective security measures, etc. The final determination of which (if any) countermeasure is to be implemented is the responsibility of the relevant O/C operation since it is ultimately their responsibility to allocate resources etc in order to accomplish the task

When considering the OPSEC process, appropriate guidance and relevant methods can also be found in ‘Security risks to Police’ of '[Managing security risks in policing]'.

Training and awareness pointers

These items should be considered when developing a user guide or presenting a training session on OPSEC.

OPSEC is a process with these five components:

Proactively released by New Zealand Police

Identify	Critical information
Analyse	Threat
Analyse	Vulnerabilities
Assess	Risk
Employ	Protective measures

This document was current as at 30 May 2022. Police policies are regularly reviewed and updated.
The most current version of Police policies are available from www.police.govt.nz

Proactively released by New Zealand Police

Planned operations

Security instructions

If we fail to meet our security obligations, our people may be harmed and national security could even be compromised. It is everyone's responsibility to ensure official Police information is protected and that operation orders are kept in safe custody. See also 'Operation orders' in the 'Planning, control and command' chapter.

Principal sources for adverse information gathering

This table shows the principal sources from which a subject(s) or suspect(s) may attempt to derive information.

Source	Comment
	s.6(a) OIA

Proactively released by New Zealand Police

s.6(a) OIA

Commencing written orders

The planning for large, diverse, expensive, or complex programmes of activities or operations requires OPSEC considerations and applications, with monitoring of those measures being incorporated. OPSEC measures associated with a major operation are the responsibility of the operations commander.

The planning and execution of smaller programmes or operations, not warranting formal establishment of a planning officer, must also take account of OPSEC considerations.

Security should enhance and enable an operation and its effectiveness not constrain it

s.6(a) OIA

An initial threat assessment should be completed in time for consideration during the operation commander's initial concept for operations and must be available prior to detailed operational planning.

Orders groups

Strictly adhere to the 'need-to-know' principle for all plans, but ensure the information is distributed widely enough to enable all those involved to carry out their roles effectively.

Proactively released by New Zealand Police

Operation commanders decide which employees ‘need-to-know’ and issue deployment orders to all those involved in the operation. Where applicable, deployed employees must be briefed on:

- The threat (this should cover all phases of the operation and all areas involved)
- Security and control of information, including documents
- Security of firearms and ammunition
- The security risk inherent in conversation with members of the public prior to, during and after operations
- The need to be alert and to report suspicious activity
- Communications security.

If an operation was developed or incorporated material from classified information, at the conclusion of that operation, the individually numbered and distributed classified copies of any operation orders must be returned to, and accounted for, by the operation commander.

See also: 'Planning, control and command' in respect of security for operation orders.

Proactively released by New Zealand Police

Security of documents during operations

General

Protecting documents from unauthorised access, disclosure or loss is dependent on the proper application of:

- clear and detailed security orders
- physical security measures
- appropriate protective markings
- the ‘need to know’ principle

Note: Even if a person has all the necessary official approvals (security clearance level) to access certain information, they should not be given access to such information, or be read into an operation, unless they have a specific ‘need to know’; that is, access to the information must be necessary for the conduct of their official duties. As with most security mechanisms, the aim is to make it difficult for unauthorised access to occur, without inconveniencing legitimate access. Need-to-know also aims to discourage browsing of sensitive material by limiting access to the smallest possible number of people. Rank does not over-rule the ‘need to know’.

Safeguarding operational documentation and material

Some safeguards are:

- displays of protected information, such as screens for boards and maps, briefing notes, charts, tables etc, must be mounted in such a manner that they cannot be seen by anyone who is not authorised to have access to them and kept secure when not attended. Consider the use of drop sheets for covering the displays when not required
- controlled access to operations rooms/areas containing operational documentation and material
- protectively marked documents, which are not in use but still required must be held in locked secure approved containers
- keys or safe codes must be safeguarded.

Loss or compromise

The loss, compromise, or suspected compromise of a document must be reported immediately. See 'Reporting security incidents' in 'Personnel security'.

Proactively released by New Zealand Police

Appendix A - Checklist of operation security matters

This checklist sets out the operation security matters that should considered as soon as an operation is initiated.

Note: The list is not exhaustive, nor will items apply under all circumstances.

Proactively released by New Zealand Police

s.6(a) OIA

Proactively released by New Zealand Police

Add additional items as required

Printed on : 30/05/2022

This document was current as at 30 May 2022. Police policies are regularly reviewed and updated.
The most current version of Police policies are available from www.police.govt.nz