

HPOL#16
Fraud Management

(Version 1.0)

Table of Contents

16.1.	SCOPE AND OBJECTIVES	2
16.2.	POLICY STATEMENT	3
16.2.1.	FRAUD DETECTION AND INVESTIGATION	3
16.2.1.1.	Fraud Risk Assessment and Analysis	3
16.2.1.2.	Strategy Definition	3
16.2.1.3.	Organizational Development	4
16.2.1.4.	Reporting of Fraudulent Activities	4
16.2.1.5.	Investigation of Fraudulent Activities and Subsequent Action	5
16.2.1.6.	Fraud Response Plan	5
16.2.1.7.	Business Aspects of Fraud Management	6
16.2.1.8.	Fraud Detection and Escalation	6
16.2.1.9.	Fraud Prevention	7

16.1. SCOPE AND OBJECTIVES

The government organization is, and wishes to be seen by all as being, honest and opposed to fraud in the way it conducts its business. The government organization is also committed to protecting its information assets from any attempt to gain by deceit, financial or other benefits, either by its own employees or members of the public, contractors, sub-contractors, agents, or intermediaries.

This policy sets out the government organization's policy towards the detection and investigation of fraud and other similar irregularities.

16.2. POLICY STATEMENT

16.2.1. FRAUD DETECTION AND INVESTIGATION

16.2.1.1. Fraud Risk Assessment and Analysis

16.2.1.1.1. A process must be developed and implemented to identify fraud sensitive areas and assess the likelihood and impact of various types of frauds.

Explanatory Notes

Areas vulnerable to fraud must be identified along with the probability of and impact of fraud. This process must include the following activities as a minimum:

- *Risk Identification: Determining what is at risk and from what sources.*
- *Risk Measurement: Determining the consequences of the risk (and to a lesser extent, the likelihood of its occurrence).*
- *Risk Prioritization: Determining the appropriate resources to manage the risk.*

16.2.1.2. Strategy Definition

16.2.1.2.1. The government organization must develop a fraud management strategy defining the government organization's plan to address fraud related issues and successful deployment of fraud management controls.

16.2.1.2.2. The government organization is responsible for instituting and maintaining a fraud management strategy supported by a system of internal control.

Explanatory Notes

The objective of maintaining a fraud management strategy supported by a system of internal control is to provide reasonable assurance for the prevention and detection of fraud, and other irregularities related to the government organization's information systems and information assets. This system of internal control will encompass all ICT processes.

- 16.2.1.2.3. Processes must be developed and implemented to provide a means for reporting fraudulent practices and for protecting the identity and legitimate interests of the person/s reporting the fraudulent activity.

16.2.1.3. Organizational Development

- 16.2.1.3.1. The ownership and responsibility for fraud management must be defined.

Explanatory Notes

A fraud management team must be created having defined roles and responsibilities for the detection and prevention of fraud.

- 16.2.1.3.2. The fraud management team must continuously obtain information related to fraudulent activities affecting institutions on an international basis.

Explanatory Notes

This information will be used to assist the government organization in detecting and preventing the occurrence of such frauds at the government organization.

- 16.2.1.3.3. The government organization must arrange for awareness workshops and seminars for all relevant personnel to give them insight on the causes and occurrence of frauds, fraud detection and escalation procedures, and punitive actions.

16.2.1.4. Reporting of Fraudulent Activities

- 16.2.1.4.1. All users of the government organization's information systems are required to report any fraudulent activity that they may identify.

- 16.2.1.4.2. Internal controls must be implemented to prevent and detect fraudulent activity.

Explanatory Notes

Processes must be developed and implemented to continuously or periodically monitor the output of these control mechanisms for the occurrence of fraudulent activities.

16.2.1.5. Investigation of Fraudulent Activities and Subsequent Action

16.2.1.5.1. It is the government organization's intent to fully investigate any suspected acts of fraud, misappropriation or other similar irregularity related to its information assets.

Explanatory Notes

An objective and impartial investigation will be conducted regardless of the position, title, and length of service or relationship with the government organization, of any party who might be or becomes involved in or becomes/is the subject of such investigation.

16.2.1.5.2. The government organization will cooperate with law enforcement agencies, in the investigation of fraudulent activities in accordance with applicable laws.

16.2.1.5.3. The government organization will pursue every reasonable effort, including court ordered restitution, to obtain recovery of losses from the offender, or other appropriate source(s).

16.2.1.6. Fraud Response Plan

16.2.1.6.1. A fraud response plan must be developed by the government organization.

Explanatory Notes

The government organization's Fraud Response Plan sets out the government organization's procedures for ensuring that all allegations and reports of fraud or dishonesty are properly followed up and progressed to their logical conclusion. These procedures must be in accordance with the government organization's Information Security Policies and in accordance with applicable laws. These

procedures must ensure that prompt and effective action is taken to:

- *Minimize the risk of any subsequent losses;*
- *Reduce any adverse operational effects;*
- *Retain evidence to assist in investigations;*
- *Improve the likelihood and scale of recoveries; and*
- *Make clear to employees and others that the government organization is not a soft target for attempted fraud.*

16.2.1.7. Business Aspects of Fraud Management

16.2.1.7.1. The government organization must analyze its business operations periodically and identify key Information Security related fraud sensitive areas.

16.2.1.7.2. The government organization must define processes to prevent, detect and manage frauds related to Information Security.

16.2.1.7.3. The government organization must set accountability for occurrences of Information Security related fraudulent activities in critical business processes and operations.

Explanatory Notes

The results of Information Security related fraudulent activities in critical business processes and operations includes but is not limited to loss of revenue to the government organization.

16.2.1.8. Fraud Detection and Escalation

16.2.1.8.1. A fraud management system must be in place and optimally configured to detect frauds and generate alarms on a real time basis.

16.2.1.8.2. The government organization must develop a fraud management plan.

Explanatory Notes

The fraud management plan will include but not be limited to procedures and corrective actions to be taken in the event of any fraudulent activity.

16.2.1.8.3. Fraud management procedure must be reviewed regularly, and updated to incorporate the changes in the business operations of the government organization.

16.2.1.8.4. The government organization must define punitive and legal actions taken against those committing or attempting to commit fraud.

16.2.1.9. Fraud Prevention

16.2.1.9.1. The controls and configuration settings of operational systems must be reviewed for any unauthorized modifications or deviation from the government organization's standard requirements.

16.2.1.9.2. All configuration settings of the operational systems must be performed in an authorized manner.

Explanatory Notes

Management of the government organization must ensure that all security and fraud preventive controls have been implemented.

16.2.1.9.3. Regular testing and simulation exercises must be carried out in order to ascertain the proper functioning of controls.