ICT Security Policy

IT Incident Management Policy

May 2013

Document Information

Master Location	:	
File Name	:	ICT Security Policy – Incident Management Policy
Distribution	:	
Author(s)	:	MoJ ICT IA

Version Control

Issue	Date	Author	Details
0-01	03/06/2011	MoJ ICT IA	Initial draft
0-02	15/06/2011	MoJ ICT IA	Revisions after ITSO review
0-03	15/08/2011	MoJ ICT IA	Revisions after internal review

Glossary and Abbreviation

Term	Definition
DSO	Departmental Security Officer
HMG	Her Majesty's Government
IA	Information Assurance
ICT	Information & Communication Technology
IT	Information Technology

RMADS	Risk Management and Accreditation Document Set
ITSO	Information Technology Security Officer
MoJ	Ministry of Justice
OST	MoJ Operational Security Team
SPF	Security Policy Framework
SIRO	Senior Information Risk Owner

References

ID	Title	Version / Issue
1	ICT Security Policy	V0-01
2	ICT Security - Technical Controls Policy	V0-01
3	ICT Security - Acceptable Use Policy	V0-01
4	ICT Security - Information Classification and Handling Policy	V0-01
5	ICT Security - IT Disaster Recovery Policy	V0-01
6	ICT Security - Forensic Readiness Policy	V0-01
7	CESG Good Practice Guide No. 24 - Security Incident Management	Issue 1.1, November 2012
8	Corporate Security and Business Continuity Branch	n/a
9	Data Access and Compliance Unit	n/a
10	Operational Security Team	n/a

References to Tier 3

ID	Title	Version / Issue
11	ICT Security Incident Management Plan and Process Guide	V0-01

Contents

1 About this document

This document is the MoJ ICT Security – Incident Management Policy. It provides the core set of ICT security principles, expectations, roles and responsibilities for IT Security incidents.

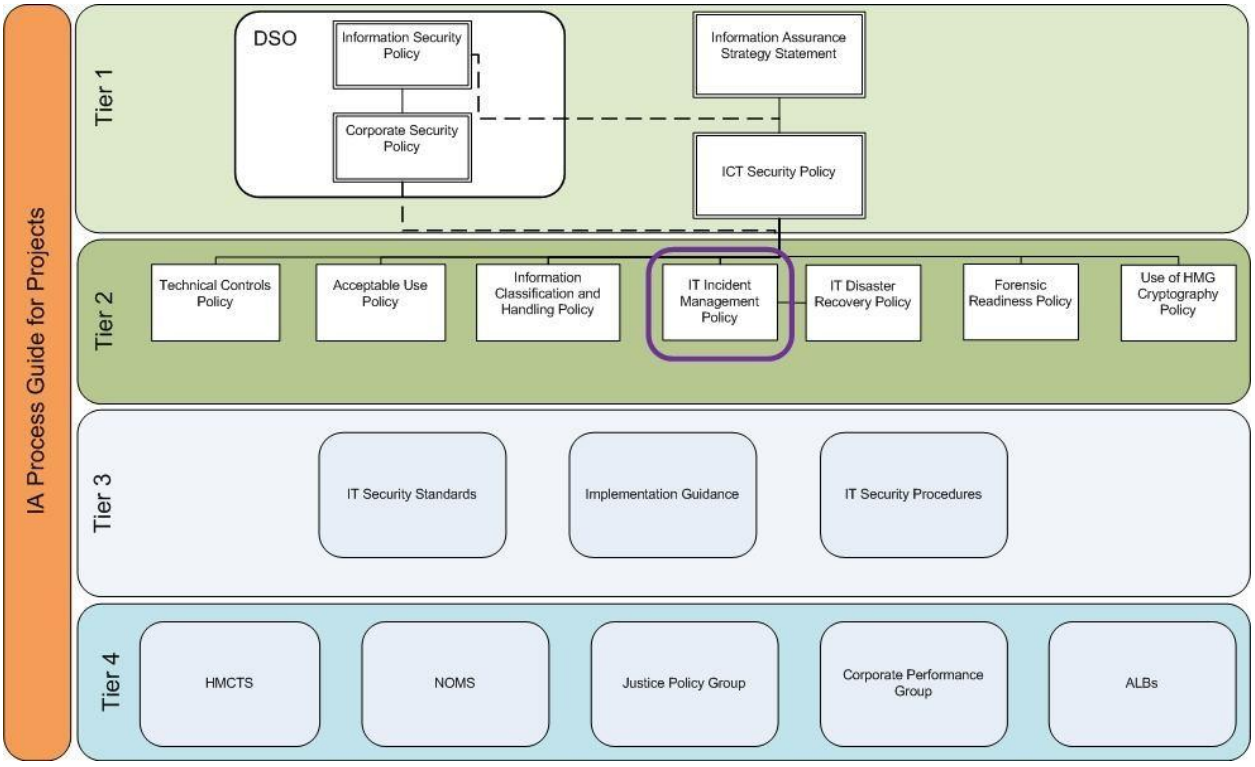

Figure 1 – MoJ ICT Security Policy Framework

1.1 How to use this document

Each policy statement outlines a security requirement and where applicable, a reference is provided to further material. A unique identifier is associated with each statement for easy reference. The format of each statement is illustrated below:

POL.ITSEC.XXX: Policy statement text.

The policies outlined in this document form the baseline standard. Where exceptions are required, this is captured on a case by case basis in Tier 4 (see Figure 1) where approval is required from both the business group SIRO and MoJ ITSO.

2 IT Incident Management Policy

2.1 Introduction

Incident management is the ability to react to security incidents in a controlled, pre-planned manner. Preparation and planning are key factors to successful information security management and all MoJ systems rely on Incident Management Plans for safe and secure operations.

The aim of this policy is to ensure best practice is followed by all IT systems when dealing with security incidents, in particular, those pertaining to data loss, in a timely and efficient manner.

POL.IMP.001: Each MoJ Business Group **must have** an IT Security Incident Management Plan which aligns to this policy. This plan must be common to all IT systems within a particular business group.

A template plan and guidance on the construction of an IT Security Incident Management Plan is provided in ICT Security – Incident Management Plan and Process guide [Ref, 11].

2.2 Scope

This policy is concerned with IT related security incidents outlining the roles and responsibilities, escalation path and criteria for escalation.

2.3 Relationship with wider MoJ functions

An IT system is one element of a number of supporting elements which sustain MoJ business functions and delivery of services. The MoJ Corporate Security and Business Continuity Branch [Ref, 8] is responsible for overall MoJ Incident Management policy and plan. This policy is designed to sit within the overall MoJ incident management structure.

3 Incident Management Process

An incident management process is a prepared course of actions that will be instigated upon the detection or report of a security incident. Incident management requires a variety of decisions to be made, drawing on the experience of a number of roles, depending on the nature of the incident.

The incident management process supports the making of informed decisions following a consistent approach designed to reduce the consequences of any incident.

3.1 Definition of an Incident

For the purposes of this policy, an incident is defined as any event or action which results in an actual and/or potential compromise of a MoJ IT asset or MoJ Information Asset (including personal data).

Such events will result in the MoJ, individuals or IT systems and/or the information held on them being exposed, or potentially exposed, to illegitimate access. As a result, incidents have the potential to compromise MoJ business delivery, the Data Protection Act, as well as the confidentiality, integrity and availability of IT systems and the information held on them. This may, in turn cause harm, distress or other damage to individuals or organisations, and result in operational disruption or reputation damage to the MoJ.

3.1.1 Types of Incidents

IT Security related incidents include (but not limited to):

- Breaches of the IT Security - Acceptable Use Policy [Ref, 3];
- Detection of malicious code (e.g. viruses and malware);
- Network attacks or Denial of Service (DOS) attacks;
- Scanning and probing of a network (where significant network resources are consumed);
- In appropriate use of MoJ ICT assets as defined in the ICT Security – Acceptable Use Policy [Ref, 3];
- The discovery of a new network vulnerability or release of a patch or software update which is considered critical or an emergency;

- The results of a penetration test on a live operational IT system that reveals critical vulnerabilities;

- Unauthorised access to an IT system;

Accidental loss of personal or other information assets;

- Deliberate release of personal or other information assets;
- Compromise of integrity;
- Any alerts or suspicious activity report generated by an IT system that proves to be a real security alert;

3.2 Incident Detection and Recording

Security Incidents may come to light from a variety of sources, including through protective monitoring solutions, reports filled by MoJ staff or breaches of the MoJ ICT Security Policy detected by an IT system.

The MoJ ICT Security Policy [Ref, 1] defines the requirements for capturing and recording security events and monitoring them for suspected malicious activity or breaches of security.

This section of the policy is concerned with taking those security events and ensuring that if an event relates to an actual IT Security incident, this incident is appropriately recorded.

POL.IMP.002:
All IT Security incidents or suspected incidents **must be** reported to the MoJ Operational Security Team (OST) within 60 minutes of detection.

POL.IMP.003:
For all incidents involving an IT Security incident, an IT Security Incident Report Form **must be** completed and submitted to the OST [Ref, 10]. This is irrespective of the reporting route (i.e. a User direct with OST or a user via the IT helpdesk).

POL.IMP.004:
All IT Security incidents involving personal data (or other information assets) **must be** reported to MoJ Data Access and Compliance Unit [Ref, 9].

The MoJ Operation Security Team (OST) is responsible for maintaining a centralised database and view of all IT Security incidents across any MoJ IT system. This database contains information on:

- Security incident reports;

- An up to date status of all reported security incidents;

  An up to date status of any actions taken with respect to a particular security incident.

This database and the effective reporting of security incidents which populate it are important in managing the MoJ's overall risk exposure. This is both in the short term, to identity any major deficiencies with an IT system which requires immediate remedial action and in the long term, to capture lessons learnt to improve Information Assurance maturity.

3.3 Categorisation of incidents

Security incidents are categorised in order to assess their impact and required level of escalation. This is to ensure that the appropriate resources can be allocated and incident resolution is conducted in a timely manner.

The three categories are:

- Low Impact (see section 3.3.1);
- Medium Impact (see section 3.3.2);

  High Impact (see section 3.3.3).

POL.IMP.005:
All IT Security incidents **must be** categorised in accordance with this policy.

The nature of an incident may not be immediately obvious when it is first reported; further assessments of its categorisation need to be made as more information is gathered. For example, through conducting an investigation (see Figure 2 which outlines this process flow).

The sub-sections below provide an overview of the three categories with further guidance on its practical application provided in ICT Security – Incident Management Plan and Process Guide [Ref, 11].

3.3.1 Low impact incident

Low impact incidents would typically be minor internal infractions, such as, a low level breach in IT Security, or, a minor loss of an IT service (e.g. due to a short loss of power).

A low impact personal data incident would typically include an incident where no actually data had been lost but a weakness in an IT system which may have

led to a potential loss is discovered where a relatively small amount of remedial action is required to address the vulnerability.

3.3.2 Medium impact incident

Examples of a medium level impact event include (but not limited to):

Deliberate disregard for the MoJ ICT Security Policy [Ref, 1] leading to minor breach in security or the potential of data loss;

- Inappropriate use of MoJ ICT assets as defined in ICT Security - Acceptable Use Policy [Ref, 2];
- Loss of data or ICT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Theft of data or ICT asset (where the data or asset is does not contain any personal data and is not protectively marked);
- Damage to any MoJ ICT asset;
- Connecting unauthorised equipment to an IT system (where there is no intent or suspicion of malicious activity);
- Prolonged or permanent failure of an IT system;
- Prolonged set of unsuccessfully attempts to scan an IT network or instigate a denial of service attack;
- Any alert or reported suspicious activity on an IT system (note this may need to be escalated to High Impact upon investigation);
- Compromise of integrity;
- The recognition of a new critical security vulnerability in an IT system (this may be the result of a penetration test);
- The release of a critical patch by an application or IT equipment vendor;
- Localised report of malicious code (e.g. the detection of a virus or malware of a desktop terminal);
- Serious case of equipment theft;
- The theft or loss of HMG cryptographic material.

3.3.3 High Impact Incident

IT Security incidents at this level require immediate escalation to the relevant MoJ Business Group Senior Information Risk Owner (SIRO) in addition to the OST and where applicable, MoJ Data Access and Compliance Unit [Ref, 9]. Incident at this impact may warrant forensic investigation.

Examples of incidents at the level include (but are not limited to):

- Evident of malicious activity, intent or espionage;

  An incident which comes to the attention of local or national media;

- Any successful network intrusion;
- Widespread malicious code attacks (e.g. a worm spreading across an IT system);
- The release of an emergency patch by an application or IT equipment vendor;
- The theft or loss of personal or protectively marked data from an IT system.

3.3.4 Further escalation requirements

The decisions to escalate an incident irrespective of its impact up through the chain from ITSO, MoJ SIRO, DSO, and above (possible to Ministerial level) may include the following factors:

- Issues of national security;
- If the incident has received local/national press coverage;
- If the incident has caused harm to a member of staff or public;
- There is high likelihood that the MoJ has suffered reputational damage or been brought into disrepute;
- Where there is a HMG requirement to report to another Department or central management function (e.g. GovCERT for network incidents or CINRAS for incidents involving HMG cryptographic material);
- Where there is a significant actual or possible loss of personal information where the Information Commissioner’s Office and Cabinet Office need to be informed.

4 Incident Management Stakeholders

This policy outlines the general incident management stakeholders and escalation path principles. Each MoJ business group implementation of this policy (which is the creation and acceptance of an IT Security Incident Management Plan) will need to consider how this is practically implemented, all the individual stakeholders involved (including others such as ICT suppliers), and escalation path.

4.1 All MoJ staff (including contractors and agency staff)

It is important that all MoJ staff are aware of what a security incident is and how to correctly report it.

POL.IMP.006:
All MoJ staff **must report** any concerns that the MoJ ICT Security Policy [Ref, 1] is not being followed to their line manager.

POL.IMP.007:
All MoJ staff **must report** any breach of the MoJ ICT Security Policy [Ref, 1] as an IT Security incident.

POL.IMP.008:
All MoJ staff **must report** any suspicious activity which indicates an IT Security incident has occurred.

POL.IMP.009:
All MoJ staff **must report** an IT Security incident either to the IT helpdesk or directly to the MoJ Operational Security Team using an ICT Security Incident Report Form.

4.2 MoJ Senior Managers

POL.IMP.010:

All MoJ Local Managers **must ensure** that all IT Security or personal data incidents or breaches are reported and taken seriously. These include facilitating any investigation and, where appropriate, pursue disciplinary action and/or legal proceedings.

4.3 Senior Information Risk Owner (SIRO)

POL.IMP.011:
Each MoJ business group SIRO **must ensure** that each ICT domain (e.g. DISC or OMNI) which fall under their remit has an IT Security Incident Management Plan which implements this policy. A template plan and guidance is available in ICT Security – Incident Management Plan and Process guide [Ref, 11].

POL.IMP.012:
All High impact IT Security incidents and any IT Security incident involving personal data **must be** reported to the SIRO immediately.

4.4 Information Asset Owner (IAO)

The role of an IAO is to understand what information is held, how it's adapted, used, shared and removed from an IT system.

POL.IMP.013:
All IT Security incidents involving the loss, theft or compromise of an Information Asset **must be** reported to the asset's IAO.

4.5 MoJ Operational Security Team (OST)

The OST are responsible for:

- Incident ownership, monitoring, tracking and communication
- Sanction enhanced monitoring on IT systems where appropriate
- Update the incident management database with details of all incidents, any investigation conducted and actions undertaken
- Carry out analysis of security incidents as required

- Initiating a forensic investigation and commissioning forensic analysis (in accordance with IT Security – Forensic Readiness Policy [Ref, 6])

  Providing progress reports on specific incidents to relevant parties.

4.6 Helpdesk

The IT helpdesk plays a crucial role in ensuring security incidents are correctly reported and escalated to the OST in a timely manner. The majority of IT Security incident will be reported to the IT helpdesk first. Also, the IT helpdesk can help identify where a user reporting an issue is actually an IT Security incident. It is therefore important that the IT helpdesk recognise this and report it to the OST.

POL.IMP.014: Where the IT helpdesk receives a report of a security incident, this **must be** reported and escalated to the OST immediately.

4.7 Escalation Path

As a rule, all IT Security incidents are reported to OST. As depicted in Figure 2, OST then progress the incident according to its categorisation (see section 3.3). Depending on the category and nature of the incident, this can involve escalating the incident to other stakeholders.

POL.IMP.015: Each IT Security Incident Management Plan **must include** a pre-arranged escalation path where each stakeholder is named and aware of their role in the Incident Management Plan.

A generic escalation path is provided in section 8. This generic path is intended to provide a starting point where further guidance on tailoring and customisation is provided in the ICT Security – Incident Management Plan and Process Guide [Ref, 11].

5 Investigation and Diagnosis capability

The OST is responsible for the investigation of all IT Security incidents. Where evidence gathering is required for possible disciplinary or legal proceedings, a forensic investigation may be required, further details are provided in ICT Security – Forensic Readiness Policy [Ref, 6].

In the course of investigation, the OST may:

- Investigate incidents at the direction of the ITSO;
- Proactively monitor suspected targets or IT systems to capture potential suspicious behaviour for analysis;
- Undertake or oversee an investigation requested by an outside agency (e.g. CESG) where authorised by the ITSO;
- Recover and securely store evidence where required;
- Require a SIRO or Senior Manager to collect more information on an IT Security incident.

POL.ITSEC.016:
The OST **must maintain** files on any investigation undertaken.

POL.ITSEC.017:
Any diagnosis of an IT Security incident and the events surrounding it **must be** shared and reported to relevant stakeholders.

5.1 Resolution, Recovery and Incident Closure

Based on the investigation of an IT Security incident, remedial action may be required to ensure appropriate incident resolution and the recovery of any IT services or information assets compromised as a result of the incident.

POL.ITSEC.018:
An IT system which has a significant compromise (Medium or High impact, see section 3.3) **must be** reported to the system Accreditor and a review of that system's risk assessment and accreditation **must be** conducted.

POL.ITSEC.019:
All IT Security incidents for an IT system **must be** collated and provided to the system Accreditor during the re-accreditation process.

5.2 Recovering from an IT Security incident

There may be occasions when it is appropriate to restore a system that has been attacked or compromised from its backup since it might be the only way to ensure system integrity.

Checks must be made to ensure the IT system being restored pre-dates the incident and does not contain any exploitable weaknesses, for example, ensure the IT system is fully patched before it is brought back into service.

POL.ITSEC.020:
The IT Security Incident Management Plan for an IT System or overarching ICT Domain **must include** details on how that system or ICT domain IT services are restored (or recovered) following an IT Security incident.

Note – The detail of how an IT system recovers from an incident event should be captured in that systems disaster recovery plan. See ICT Security – Disaster Recovery Policy [Ref, 5] for further information.

6 Preventing re-occurrences

Once the cause of an IT Security incident has been identified, steps must be taken to reduce the risk of its reoccurrence, for example eradicate any computer viruses, block firewall ports, and install any missing system patches, as necessary.

6.1 Learning points

When an IT Security incident has been resolved and closed, a management report needs to be prepared outlining the incident, the outcome of the investigation, actions taken, and recommendations about how to improve the business systems to reduce the likelihood of a reoccurrence.

Copies of the report must be sent to the ITSO who has a responsibility for forwarding the report onto any HMG central reporting functions, for example CESG, GovCertUK or CINRAS, as appropriate.

POL.ITSEC.021:
For each Medium and High impact (see section 3.3) IT Security incident, a management report must be prepared covering:

- A description of the incident;
- The outcome of the incident investigation;
- Actions raised (or taken) with associated action owners; - Any recommendations made.

7 IT Security Incident Recording and Categorisation

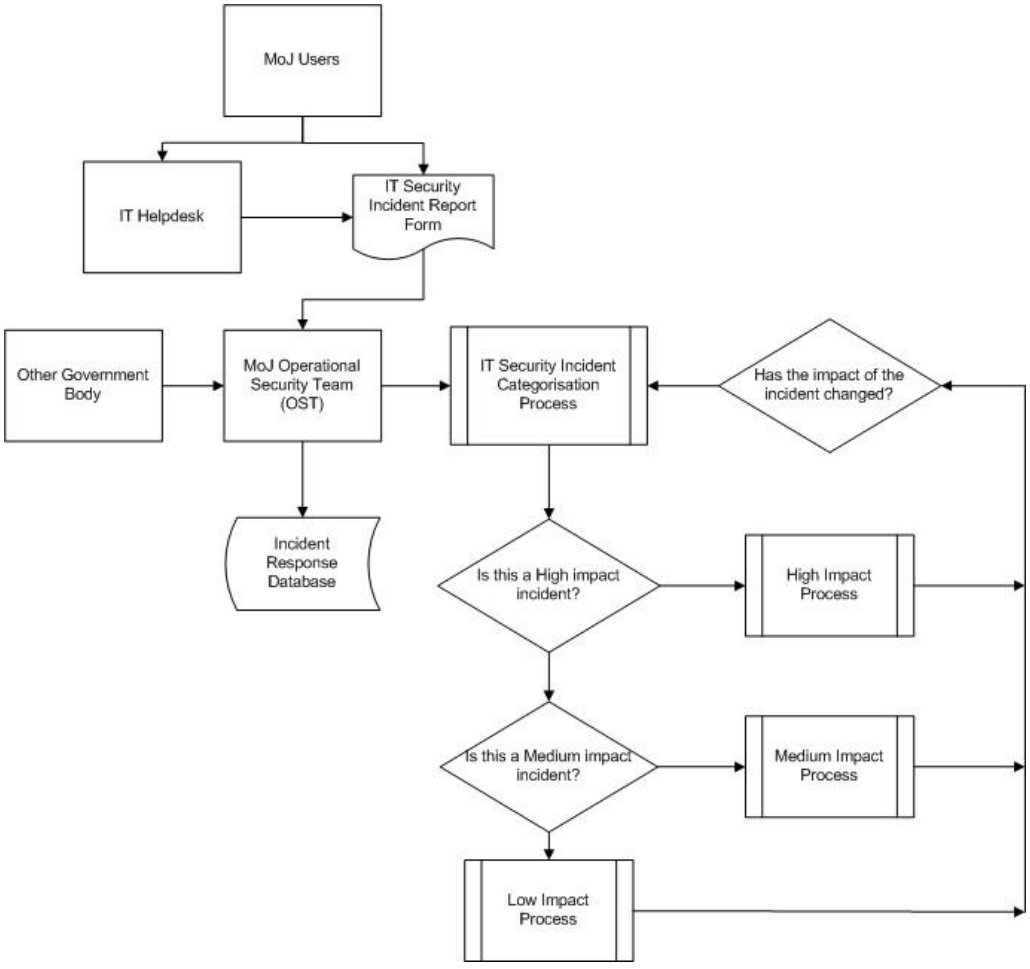

Figure 2 - IT Security Incident Recording and Categorisation

8 IT Security Incident Escalation Path

Figure 3 is a generic IT Security incident escalation path which provides a starting point for the creation of a tailored version in an IT Security Incident Management Plan. Further information is provided in the ICT Security – Incident Management Plan and Process Guide [Ref, 11].

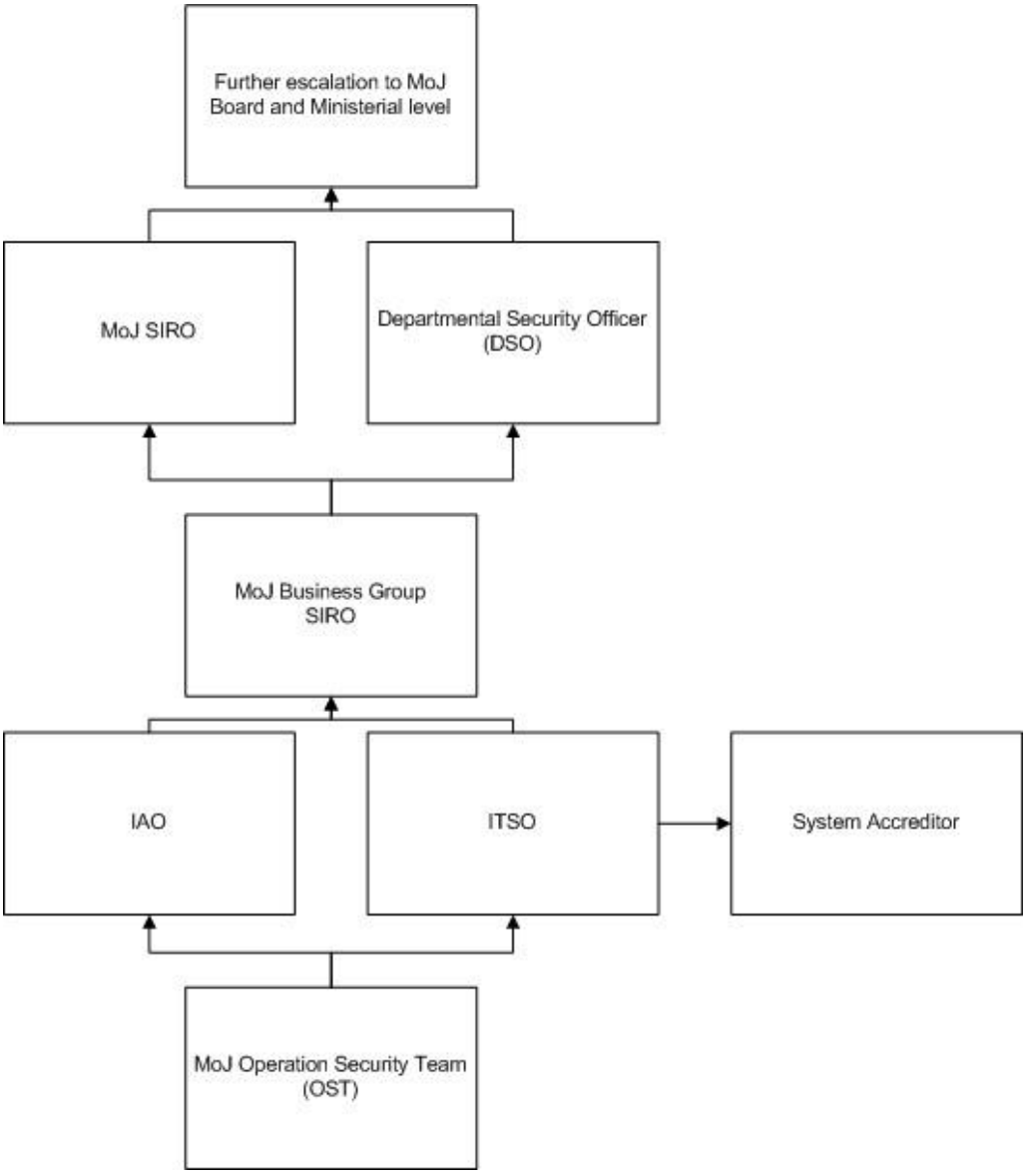

Figure 3 - IT Security Incident generic escalation path