STANDARD OPERATING PROCEDURE

Title: SOP 078: IT Information Security Incident Management		
Status: **PUBLIC**		Documents Number: **SOP/ATSEC/078**
Effective Date: **01.01.2016**		Review Date: **01. 01.2017**
SERVICE OWNER	IT Security Coordinator	DATE & SIGNATURE
LEAD AUTHOR	Marina Stavridi	DATE & SIGNATURE
APPROVER	D/Director ICTS	DATE & SIGNATURE
	Chief Infrastructure Support	DATE & SIGNATURE
	Chief Functional Support	DATE & SIGNATURE
	Chief Software Development	DATE & SIGNATURE
	IT Governance, Security and Systems Architect	DATE & SIGNATURE

PURPOSE:

This procedure defines which functional teams perform which tasks related to handling an IT Information Security Incident.

SCOPE:

This SOP defines actions to be taken in order to manage incidents threatening IT information security under the framework of the Incident Management process (SOP070) in the OSCE and in particular when

- an incident is raised for an IT event that harms, or attempts to harm, the confidentiality, integrity and/or the availability of information on the affected OSCE service(s), and thus constitutes a **security issue**.

POLICY:

This procedure reflects the applicable ITIL v3 Incident Management Process, The ICT Policy defined in Financial Administrative Instruction 12:

- VII Eligibility of Access,
- VIII Use of OSCE Computing Resources,
- IX Prohibited Use,
- X Internet Access and Security,
- XI Privacy,
- XIII Individual Responsibilities

and Financial Administrative Instruction 13:

- Chapter 2, Principles of Information Security
- Chapter 3, Responsibility for Information Security
- Chapter 5, Access to Information, paragraphs 5.1 to 5.7, 5.12, 5.13, 5.14
- Chapter 6, Standard Practices related to OSCE Information Systems, paragraphs 6.1.10, 6.2.4, 6.2.6, 6.3.1, 6.5.2, 6.5.3
- Chapter 7, Production Systems Development, paragraphs 7.5, 7.9
- Chapter 8, Control of Information Security, paragraph 8.1

IT Information Security Incident management is part of ICT Incident Management and constitutes and integral part of the ICT User Services Catalogue. It applies to all users being assigned an OSCE corporate device (asset) and/or individuals accessing OSCE information systems.

SERVICES:

This procedure relates to the following services defined in the ICT User Services Catalogue:

- Support services
- Security services
- Consulting services

SERVICE LEVEL:

This procedure applies to the incident service levels defined in SOP 070, priorities Blocking, Critical and High.

INITIATION OF PROCEDURE:

Initiation of this procedure is triggered when a new incident that constitutes an IT information security issue as defined in the Scope section above is created in the IT support ticketing tool.

PREREQUISITES:

Service Desk staff needs to have access to view all incidents related to their function in the IT support ticketing tool.
Service Desk to be aware of the applicable SLA/OLA for the particular incident and the priority level of this incident.

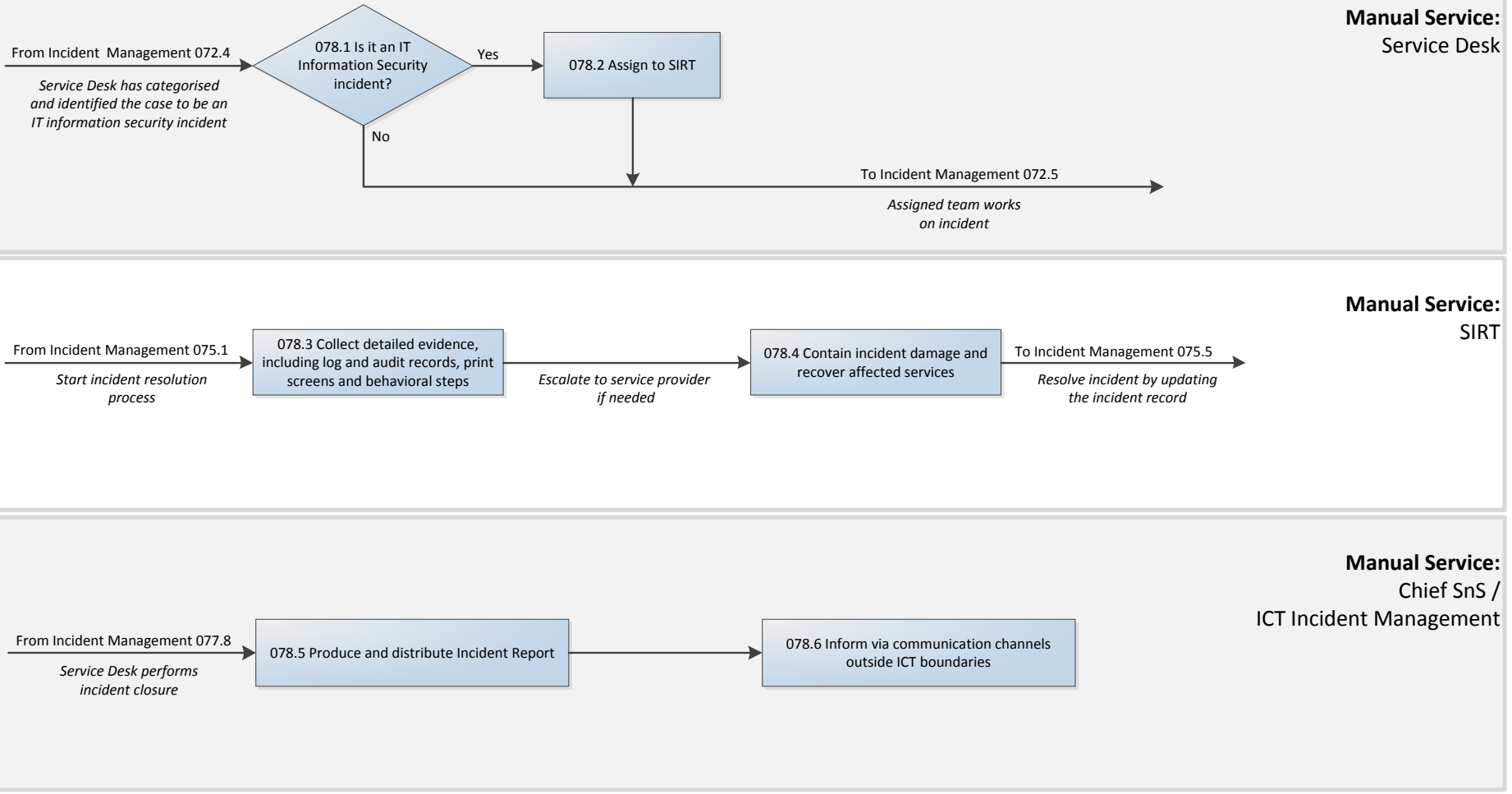
INPUTS:

New incident ticket; Applicable SLA.

PROCEDURE:

See Workflow “IT Information Security Incident Management”

SOP 078 IT Information Security Incident Management (070 Incident Management, sub-process 8)



The process is triggered when an **IT information security incident** is created in the IT support ticketing tool.

An IT information security incident is an IT event that harms or attempts to harm the confidentiality, integrity and/or the availability of information maintained within a service and thus constitutes a security issue.

Events that can trigger as IT Information Security Incidents can be of (but not limited to) the following nature:

- Malware
- An anomaly detected by the security infrastructure
- Unauthorized alteration of information including destruction of data
- Unauthorized access to classified or otherwise sensitive data
- DoS
- Unauthorized alteration of Web site contents
- Suspicion of an attack in the ICT infrastructure
- Intrusion/penetration of a system/server and compromising of its integrity

Misuse of OSCE computing resources by an employee
And can cause the following damage:

- **Loss of information availability:** Information is unavailable to all users of a service (e.g. a service is unavailable or under attack)
- **Breach of Integrity:** Information is unusable to all users of a service (e.g. corruption of data or inability to extract the data)
- **Breach of confidentiality:** Information is exposed to / shared with external parties (e.g. espionage - disclosure of sensitive information to a third party, etc.)
- **Loss of accountability services:** disruption of the process tracing the information management activities (e.g. modification or destruction of audit logs).
- **Security violation:** non-compliance with the security policy (e.g. breach of confidentiality, breach of integrity, loss of information availability, loss of accountability).

Process

When a new incident is received in the Service Desk ticketing queue, the Service Desk performs *Incident Registration* tasks (SOP 071), including gathering all necessary information for the incident record (meaningful and whole description of the problem, printscreens, etc). The SD also applies a first classification of impact and urgency of the reported issue. Equally important is to link all cases of the same behavior from different reporting users to one ticket that will track progress of the incident.

The Service Desk will follow the incident assignment process (SOP 072) and if they assess during initial investigation that the reported issue constitutes an IT information security incident as defined earlier, the SD will assign it to 'ICT-SIRT' and also call and text (SMS) the SIRT Coordinator and SD Lead.

SIRT (Security Incident Response Team)

SIRT includes the following members:

- SIRT Coordinator, SEC: Chief IT Governance, Security & Systems Architect (PKS), with Chief SnS (MS) as alternate
- ICT Platform Senior Administrator (AH), with NK as alternate
- ICT Security/Networks Senior Administrator (AO), with HH as alternate
- ICT Service Desk team lead (CR), with RR as alternate
- Executive Structure ICT designated SIRT member or ES ICT Chief, if applicable
- External Contractor/Consultant, if applicable[1]

Responsibilities of the Security Incident Response Team (SIRT)

The goal of SIRT is ultimately to stop or contain the information security breach as soon as it is detected.

SIRT shall follow the below key steps under the Incident Resolution process (SOP 075):

1. review all evidence and re-establish the fact that this is indeed a security incident;
2. gather all detailed evidence, including log and audit records, print screens and behavioral steps, which are of utmost importance for adequately analyzing, recovering from and preventing re-occurrence;
3. analyze the symptoms and identify the cause;

It is **important to note** that:

- SIRT shall not tamper with or destroy evidence during investigation

[11] Contracted consultants may take part to the investigation with designated responsibility assigned by the SIRT Lead.

- SIRT shall take immediate action in order to contain the incident, including removing equipment from the network or disabling user accounts.

4. perform incident containment;
5. escalate if needed; (e.g. from local ICT to SEC ICT);
6. plan and implement corrective action;
7. advise on steps moving forward so as to prevent recurrence, if necessary;
8. communicate with those affected by or involved with recovery from the incident;
9. report the action to the ICT Incident Management team as soon as possible.

Audit trails and similar evidence shall be collected and secured, as appropriate, for:

1. internal problem analysis;
2. use as forensic evidence in relation to a potential breach of contract or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
3. negotiating for compensation from software and service suppliers.

Incident tracking and follow up is performed according to SOP 074; in this aspect, the Service Desk team leader, also member of the SIRT, is responsible for maintaining the incident record on regular basis and feeding appropriate information to relevant internal ICT audience as described in the next section.

Incident Functional Escalation (SOP 076) and Incident Closure (SOP 077) procedures apply as is for Major Incidents, including Incident Report (compiled by the SIRT Coordinator) to be produced two working days after incident closure.

IT information security incident communication

The decision and responsibility of whether -and to whom- to communicate an IT information security incident outside ICT boundaries falls into the responsibility of the ICT Incident Management team, as this is defined in SOP 074.

In respect to the Information Security incident process, the ICT Incident Management team comprises from its original members:

- Deputy Director for ICT Services (acts as team lead)
- IT Governance, Security and Systems Architect
- ICT Infrastructure and S&S Chiefs
- ICT Service Desk lead
- ICT Network and Server leads

plus

- IT Security Co-ordinator, in the case of an IT information security incident.

In terms of communication management of an IT major information security incident, the following should apply:

- ✓ Any IT member identifying an Information Security Incident is responsible to inform the local Service Desk Lead and ICT Chief.
- ✓ The Local ICT Chief is responsible to escalate immediately to SIRT and inform the ICT Incident Management team.
- ✓ The SIRT Coordinator is responsible to produce the initial Incident Report and distribute it to ICT Incident Management.
- ✓ SIRT is responsible to ensure that the Incident Management team is informed of the information security incident as soon as possible and should endeavor to contact at least one of its participating managers in sms or phone.

Learning from security incidents

The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.
As part of continual service improvement, the ICT Incident Management Team perform a post mortem evaluation that may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or taken into account in the security policy review process (acceptable risk).

These measures should be documented, communicated to the senior management and regularly followed up for implementation.

OUTPUTS:

The affected user(s) are provided with:

- Incident resolution.

SIRT conducts:

- Incident analysis and resolution;
- Regular progress updates according to the Major Incident Communication procedures described in SOP 074.

ICT Management is provided with:

- Incident Report (including lessons learned)

RESPONSIBILITIES:

R= Responsible, A= Accountable, C= Consulted, I= Informed

Task	Reporting User	Local Service Desk	Chief S&S	SIRT	SIRT Coordinator	SD lead / Chief ICT	ICT Incident Management
Submits new information security incident Reports cases of FAI13 non-compliance regarding misuse of OSCE information systems	R, A	I				I	
Classifies information security incident		R				A	
Escalates information security incident		R		I		C, A	I
Coordinates SIRT activities					R	I	
Communicates resolution updates			I		R	I	I
Follows up information security incident progress and ensures incident record is regularly updated		I	A	C		R	
Resolves information security incident		I	I	R	A	I	I
Communicates resolution to reporting user(s)	I	R	I			A	I
Produces and communicates Incident Report				I	R, A	I	I
Communicates outside ICT boundaries			C, I			C, I	R,A

ESCALATIONS:

Escalations will be handled by the service owner in accordance with the Incident Management Process Procedure 073 “Complaint Handling” and Procedure 076 “Incident Escalation Handling”.

Incident	Escalate to
User complaint	Chief S&S and mission IT Head
IT information security incident	ICT Incident Management

REFERENCES

- ITIL v3 Incident Management Process
- Incident Tracking procedure
- Incident Analysis and Resolution procedure
- Incident Escalation handling procedure

AUDIT TRAIL

Incident record:
The user’s request, the date it was received, the corresponding SIRT actions taken, correspondence with the reporter, the incident management outcome, the log of SIRT work, are logged in the corresponding ticket in the IT support ticketing tool.

Referenced documentation:
The official versions of referenced documentation will be maintained on DocIn.

DEFINITIONS
(applicable to ITIL v3)

IT Information Security	The term ‘information’ is used as a general term and includes data stores, databases and metadata. The goal of IT information security is to guarantee safety of information, meaning its confidentiality, integrity and availability, into IT systems and services made available by the organization.

Failure	Loss of ability of a service to operate to the agreed levels or to deliver the agreed output.
IT service	A service provided to one or more users by ICTS or mission/delegation IT. An IT service is based on the use of Information Technology and supports the OSCE business processes. An IT service is made up from a combination of people, processes and technology and should be defined in a Service Level Agreement.
Incident	An unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident. For example, failure of one disk from a mirror set.
Incident Management	The process responsible for managing the lifecycle of all incidents. The primary objective of Incident Management is to return the IT service to users as quickly as possible.
Service Desk	The single point of contact in ICT for OSCE staff members, Delegations, members of the general public using iRecruitment and consultants using ICT services. The Service Desk handles incidents and service requests and also handles ICT communication to service users.
Impact	A measure of the effect of an incident, problem or change on the affected business process. Impact and urgency are used to assign priority.
Urgency	Measure of business criticality of an incident, problem or change where there is an effect upon business deadlines. The urgency reflects the time available for repair or avoidance before the impact is felt by the business. Together with impact, it is the major means of assigning priority for dealing with incidents, problems or changes.

REVIEW PERIOD

Yearly or when a major change is performed on underpinning policies.