ICT SECURITY INCIDENT MANAGEMENT GUIDELINES

VERSION 1.2

08 JUNE 2018

Table of Contents

1. INTRODUCTION

The South African Public Service transformation is, at a strategic level, informed by public service-wide strategic priority areas and is guided by principles of equal access to services, increased productivity and lowering of costs. In this regard the continuance of the business of government in support of service delivery, thus business continuity, is of utmost importance.

As government is the custodian of extensive information holdings it relies upon its information assets for fiscal, policy and service delivery initiatives.

In recent years ICT has become integral to many of the essential activities carried out by institutions. The advent of the Internet and other electronic networking services together with the current and developing capabilities of systems and applications also meant that institutions have become more and more dependent on reliable, safe and secure ICT infrastructures.

The management of electronic information requires government to protect the integrity and availability of the information assets in its care. As information is the backbone of the achievement of business objectives and government service delivery, security breaches to integrated government services can cause crippling effects to the service delivery, with major inconveniences to the users of services.

To derive value from ICT as a strategic resource is not achievable in absence of or within a weak secure ICT environment that fails to ensure the confidentiality, integrity and availability of information within the underlying ICT systems. Achieving ICT security requires an effective management of risk, which encompasses risks from physical, human and technology related threats associated with all forms of use and or processing of electronic information within the institution.

To understand the risk profile of the South African Government it is necessary to understand the underlying vulnerabilities impacting on ICT security. It is therefore necessary to establish related mechanism to prepare for, detect and respond to information security threats and incidents.

2. PURPOSE

No matter the extent of our defenses, it inevitable that Information Security Incidents will occur. For this reason establishing, periodically assessing, and continually improving incident management processes and capabilities is very important. This guideline intends to provide guidance to institutions to prepare for, detect and respond to and report on information security threats and incidents.

3. SCOPE OF APPLICATION

This guideline provides a structured and planned approach to incident management within institutions:

a) Detect, assess and mitigate electronic information security vulnerabilities and incidents;

b) Report on electronic information security incidents; and

c) Continuously improve electronic information security and incident management as a result of managing information security incidents and vulnerabilities.

4. LEGAL FRAMEWORK

4.1. **Section 3(1) of the Public Service Act (PSA) of 1994,** as amended, mandates the Minister for Public Service and Administration (MPSA) to establish norms and standards that inform proper management and functioning of national and provincial departments.

4.2. These norms and standards referred to in **Section 3(1)** include *inter alia* matters relating to the optimal utilisation of IT as a valuable and scarce resource.

4.3. **Chapter 5 (Part II) of the Public Service Regulations**

Information security vigilance

(1) A head of department shall ensure the maintenance of information security vigilance at all times in the department; and

(2) When non-compliance with the Information Security Standards referred to in regulation 92(1) comes to the knowledge of an employee of a department, he or she shall report it immediately to the head of department or an employee designated for this purpose by that head.

Incident reports

A head of department shall regularly, on the basis of the threat posed by an incident, submit to the Director-General: State Security Agency, the Auditor-General and such other authorities as the head considers appropriate-

(a) An incident report of every instance of non-compliance with the Information Security Standards referred to in regulation 92(1); and

(b) A plan on how incidents of non-compliance will be corrected and how to prevent similar incidents in future.

4.4. Minimum Information Security Standards (MISS) Chapter 9

i. Heads of security or those tasked with the security responsibility of an institution must report all instances of a breach of security / incidents, or failure to comply with security measures, or conduct constituting a security risk, as soon as possible to the Chief Directorate Security of the National Intelligence Agency, and where appropriate to the SAPS (Crime Prevention Unit) or the SANDF (MI) (see Appendix A). Where official encryption is concerned, a security breach must also be reported to COMSEC;

ii. When a breach of security occurs, the existing channels must be used to report it. It is the responsibility of the head of the institution to ensure that all breaches of security

are reported; and

iii. Breaches of security must at all times be dealt with using the highest degree of confidentiality in order to protect the officer concerned and prevent him or her from being unnecessarily done an injustice to.

5. INCIDENT MANAGEMENT

An information security incident is defined as any unauthorized action taken on government electronic information assets that reduces, compromises, or threatens the confidentiality, integrity, availability, or non-repudiation of the data or systems themselves. This includes, but is not limited to, the following:

- Removing or bypassing existing protection and control mechanisms;
- Using or misusing control mechanisms to gain or grant unauthorized access or system privileges; or to escalate current privileges;
- Reading, copying, modifying, or deleting data by an individual or program not authorised for such action;
- Abusing privileged access in order to monitor or impersonate another user, or reading that individual's private data without authorisation;
- Accidental or deliberate unauthorised change of data;
- Attempting to explore or test for security vulnerabilities in information assets when not authorised to do so; and
- Any violation of a security policy.

As a key part of an institution's overall information security strategy, the institution should put controls and procedures in place to enable a structured well planned approach to the management of information security incidents. The primary steps to minimise the direct negative impact of information security incidents are the following:

- Stop and contain;
- Eradicate;
- Analyse and report; and
- Follow up.

Information security incident management guidelines identify mechanisms to detect and report when information security events occur and the directives for the consistent management of such events. The information collected about the events can be analysed to identify trends and to direct efforts continually improve and strengthen the information security infrastructure of the institution.

6. INCIDENT MANAGEMENT PROCESS

As a key part of an institution's overall information security strategy, the institution should

put controls and procedures in place to enable a structured well planned approach to the management of information security incidents.

All incidents such as security related environmental changes or software malfunctions with the potential to disrupt network traffic or operational systems, or threaten confidentiality, integrity or availability of any component of an institution or government information system should be reported on the Help Desk who should escalate all high impact incidents to the Institution Security Officer and related management as soon as possible so that prompt remedial action can be taken.

All institution employees, IT staff, external parties, contractors and temporary staff should be made aware of the security incident reporting procedure and that they are required to report any security incidents and malfunctions as soon as possible.

The Help Desk is responsible for maintaining an incident register which will include details such as incident category and severity level, logging date, review, escalation etc. where all security incidents are recorded.

All system owners should report all significant security-relevant environmental changes promptly to ICT management. Such changes include changes of physical access means, changes of security responsibilities and changes of established security measures.

The relevant management should ensure that all open incidents and actions against open security incidents and weaknesses are reviewed and monitored weekly.

Security incidents and malfunctions need to be resolved and closed by IT staff and / or management in a timely manner consistent with documented response procedures.

The Help Desk should provide feedback to individuals who reported the security incident and notify them of results.

Mechanisms enabling types, volumes and costs of security incidents to be quantified and monitored should be in place to assist in identifying recurring or high impact incidents or malfunctions, as well as mitigating actions to prevent the recurrence or future impact of similar incidents.

It is the Director-General's responsibility to decide whether or not to inform law enforcement in the event of a security incident where any breach of statute may have occurred.

6.1 Incident Categorisation

Categorisation of information security incidents is important for the information security incident management process. Categorisation creates structure in the collection of all possible information security incidents that an institution may face at some point in time.

Response procedures to address security incidents should be documented indicating what actions and escalation needs to be taken in the event of security incidents. The table below serves as guidance to institutions on categorisation of incidents:

Table 1: **Incident Categories (Adapted from SITA and SSA Incident Reports)**

IT Security Incident	IT Security Related risk(s)
Access control	• Creation or deletion of unexpected user accounts • High activity on a previously low usage or idle account • Inability to login due to modifications of account • Unexpected change of user password • Unusual time of usage • A suspicious last time login or usage of a user account • Unusual usage patterns (e.g. Programs are being compiled in the account of user who is not involved in programming) • Operating system security alerts (ie.multiple logons, password changes, disabled and inactive accounts, etc.)
Network Security	• Alerts pertaining to missing patches; • Operating system utilization alerts – For capacity management (alert when determined thresholds are exceeded) • Defacement of webpage (unauthorised alteration of the content of one or more pages of the website; and • Alerts pertaining to configuration change
Critical Asset Rooms	• Alerts pertaining to environmental conditions (temperature, humidity, fire etc.)
Equipment Security	• Intrusion Prevention Systems alerts – Alerts for Intrusion Prevention System • Theft of hardware / software
Web defacement	• Loss of reputation and information integrity
Computer Virus / Malware	• Alerts pertaining to Antivirus (AV not installed, removed or disabled),spam, network worm, Trojan horse,botnet,blended attacks, malicious programs etc
Compromise of functions and Denial of Service Attack	• Computer system becomes inaccessible without explanation • Abuse of access rights, forging of access rights, denial of actions etc
Compromise of Information	• The use of another person's identity to gain excess privilege in accessing system • ID Theft,interception,spying,eaves dropping,disclosure,masquerade,social engineering, network

	phishing, theft of data, loss of data, tampering with data, data error, data flow analysis etc.
Infrastructure failure	• Power supply failure, networking failure,airconditioning failure, water supply failure,etc
Unauthorised use of resources	• Using resources for unauthorised purposes
Copyright	• Selling or installing copies of unlicensed commercial software or other copyright protected materials
Loss of information security caused by natural disasters beyond human control	• Earthquake,volcano,flood,violent,wind,lightining,tsunami,collapse

6.2 Management of information security incidents and improvements

The first priority in responding to any security incident in institutions is to stop the security breach itself and prevent its recurrence. Where the severity of the incident and its likelihood of recurrence justify it, management can and should take any steps necessary on a temporary basis, such as removing systems from operation, revoking system accesses or removing involved personnel from institution facilities.

To address security incidents and malfunctions, a formal incident response procedure should be established setting out the action to be taken in the event on a security incident. The procedures should consider:

- The evaluation of reported security incidents and weaknesses;
- Collection and preservation of evidence related to the security incident;
- Determining actions to address the security incidents and weaknesses; and
- Monitoring progress on the actions.

6.3 Risk Alert levels, reporting and escalation

In order to ensure a coordinated handling of high level IT security incidents, it is necessary to understand and classify incidents according to specific risk levels. The following table indicates the risk alert levels as well as associated reporting to ensure the identification of a threat posture, and escalation to ensure coordination at the correct level.

Table 2: Incident Levels (Adapted from draft SSA incident reporting mechanisms)

Risk Alert Level	Alert	Report	Escalate
RED - Critical	• An incident that poses a critical risk to a government institution; • An incident that poses a critical risk to multiple government institutions; • An incident that poses a high or critical risk to any or multiple critical Infrastructure.	Helpdesk / Information Security Officer	Head of Institution
Orange - High	• An incident that poses a high risk to a government institution; • An incident that poses a high risk to multiple government institutions; • An incident that poses a medium risk to any or multiple critical infrastructure.	Helpdesk / Information Security Officer	Head of Institution
Yellow - Medium	• An incident that poses a medium risk to a government institution; • An incident that poses a medium risk to multiple government institutions; • An incident that poses a low risk to any or multiple critical infrastructure.	Helpdesk / Information Security Officer	Relevant Information Security Structures within an Institution
Blue - Low	• An incident that poses a low risk to multiple government institutions.	Helpdesk / Information Security Officer	Relevant Information Security Structures within an Institution
Green - Reported	• An incident that poses a low risk to a government institution.	Helpdesk / Information Security Officer	Relevant Information Security Structures within an Institution

6.4 Identifying High, Medium and Low Risk Incidents

Severity levels are utilised to rate the extent of the impact and the scale used to determine the severity that was caused by a security-incident, or that could be caused by a security-incident if the incident is not addressed appropriately. It is made up of four categories, namely Critical, High, Medium and Low.

(a) Critical Severity

A Critical severity incident would cause "exceptionally grave damage" to national security and this may lead to the occurrence of the following in some cases:

- Severing of relations between states;
- Economic losses affecting the majority of South Africans;
- A declaration of war;
- A loss in high availability of military communication systems, banking communication systems critical government infrastructure, or Critical Communications Infrastructure, essential to the daily operations of the institution and sectors of South Africa;
- Financial impact to the South African government;
- Legal ramifications for South Africa, state institutions or Sectors;
- Loss of strategic or diplomatic advantage for South Africa;
- Impact to the health and safety of the institution's staff.

(b) High Severity

High severity incident would cause "serious damage" to national security if appropriate security controls are not implemented and the severity impact referred to above may lead to the occurrence of the following in some cases:

- The state or institutions will not properly fulfil its normal functions;
- Operational co-operation between institutions is disrupted in such a way that it threatens the functioning of one or more of these institutions i.e. the Judiciary, Military, sectors and others;
- Economic losses affecting a number of South Africans;
- A loss in some availability of military communication systems, banking communication systems critical government infrastructure, or Critical Communications Infrastructure, essential to the daily operations of the institution and sectors of South Africa;
- Financial impact to the institution or South Africa is probable;
- Potential for legal ramifications for the institution concerned or South Africa is of high concern;
- Loss of strategic or diplomatic advantage for South Africa is expected;
- Impacts directly on the ability of the national institution to fulfill its mandate; and
- Potentially impacts the health and safety of the institution's staff.

(c) Medium Severity

A Medium severity incident will cause "damage" or be "prejudicial" to national security. The severity impact referred to above may lead to the occurrence of the following in some cases:

- Undue damage to the integrity of an area within a sector, an institution or South Africa i.e. defaced government websites, but not entailing a threat of serious damage;
- The unavailability or compromise of systems or electronic communications may frustrate everyday functions, lead to an inconvenience and bring about wasting of funds;
- The orderly, routine co-operation between Sectors, institutions, countries and/or individuals may be harmed or delayed, but not bringing functions to a halt;
- A potential loss in some availability of military communication systems, banking communication systems critical government infrastructure, or Critical Communications Infrastructure, essential to the daily operations of the institution and sectors of South Africa;
- Potential financial impact to a sector, institution or South Africa;
- Potential for legal ramifications for a sector, institution or South Africa;
- Potential loss of strategic and diplomatic advantage for an institution or South Africa; and
- Embarrassment for the Sector, institution or South Africa.

(d) Low Severity

A Low severity incident could cause possible "damage" or possibly be "prejudicial" to national security. The severity impact referred to above may lead to the occurrence of the following in some cases:

- Possible impact to the integrity of an area within a sector or an institution i.e. virus or malware outbreaks that can be controlled, but not entailing a threat of damage;
- The possible unavailability or compromise of systems or electronic communications that may frustrate everyday functions, lead to an inconvenience and bring about wasting of funds;
- The orderly, routine co-operation between Sectors or institutions may be delayed, but not bringing functions to a halt;
- Potential minor financial impact to a sector or institution;
- Potential for minor legal ramifications for a sector or institution; and
- Potential Embarrassment for the Sector or institution.

NOTE: During a complex incident, the executive powers may choose to activate other national security alerts etc. depending on the severity, magnitude, or scope of an incident.

6.5 Training

It is essential to provide adequate training to ensure all concerned staff and management are capable of handling security incidents. Staff should be familiar with the procedures to handle the incident from incidents identification reporting, and taking the appropriate actions to restore the system to normal operation. Drills on incident handling should also be organised regularly for staff to practice the procedures.

In addition, sufficient training to system operation and support staff on security precaution knowledge is important, in order to strengthen the security protection of the system or functional area, and reduce the chance that an incident may occur.

6.6 Incident Monitoring and Measures

A sufficient level of security measures for incident monitoring should be implemented to protect the system during normal operations as well as to monitor potential security incidents. The level and extent of measures to be deployed will depend on the importance and sensitivity of the system and its data, as well as its functions.

Service providers should ensure that all security incidents and weaknesses are promptly reported to the relevant authority and that appropriate action is taken.

Listed below are some typical minimal measures for security incident monitoring:

i. Install firewall device and apply authentication and access control measures to protect important system and data resources;

ii. Install intrusion detection tool to proactively monitor, detect and respond to system intrusions or hacking;

iii. Install antivirus tool and malicious code detection and repair tool to detect and remove computer virus and malicious codes, and prevent them from affecting system operations;

iv. Perform periodic security check by using security scanning tools to identify existing vulnerabilities;

v. Install content filtering tool to detect malicious contents or codes in emails or web traffic;

vi. Enable system and network audit logging to facilitate the detection and tracing of unauthorised activities; and

vii. Develop programs and scripts to assist in the detection of suspicious activities, monitoring of system and data integrity and analysis of audit log information.

Conclusion

Each department involved in a security incident will play a unique response role. Each has a distinct mission and different authorities, so response actions will differ. However, all partners have the responsibility to maintain, at minimum, the following capabilities during the response phase:

- All departments should have the ability to gain and maintain situational awareness about the performance of any unauthorized activity on their networks and communications systems.
- Information based on this awareness should be passed to the Cyber Security Centre directly or through previously established reporting channels to help inform the national picture.
- SSA and the Cyber Security Centre will assist departments in ensuring that they understand what type of information needs to be shared throughout the incident response cycle. Necessary response resources should be readily available and should be based on each department's security response plans as informed by this plan. This includes notifying and activating security response organizations, plans, and personnel and requesting assistance when needed.
- All departments should notify pre-identified IT and ICT security staff and senior officials and make them available to the Cyber Security Centre and/or other operations centres as needed upon request of the SSA.
- During the course of the incident, departments that may have responded under their own authorities should notify the Cyber Security Centre and coordinate further actions as part of the national response effort. Once the Cyber Security Centre receives additional reporting, it notifies appropriate security incident stakeholders of the situation and continues to coordinate required and requested response activities.
- It further must be stated that this draft security incident mechanism is a living document and will be amended from time to time as it matures or in line with changes to the environment, strategy or approach. This procedure manual / mechanism shall be reviewed annually and/or when a need arises. Any latest relevant legislations, internal policies and procedures shall be taken into account when reviewing this manual procedure.

7. REFERENCES

[1] South Africa. Minimum Information Security Standards (MISS) of 1996

[2] South Africa. Public Service Regulations, Chapter 5 Part II, 2001 - Government Notice No. R.1 of 5 January 2001

[3] SANS 27035: 2013 Information Technology – Security Techniques – Information Security Incident Management (www.sabs.co.za)

[4] South Africa: Western Cape Information Security Incident Management Standard

[5] SANS 22301: Business Continuity – Societal Security – Business Continuity Management Systems (www.sabs.co.za)

[6] SANS 24762: Information Technology – Guidelines for information and Communications Technology Disaster (www.sabs.co.za)

[7] SANS 27004: Information Technology – Information Security Management – Measurement (www.sabs.co.za)

[8] SANS 27005: Information Technology – Security Techniques – Information Security Risk Management (www.sabs.co.za)

[9] SANS 27007: Information Technology – Security Techniques – Guidelines Information Security Management Systems Auditing (www.sabs.co.za)

[10] SANS 27033: Information Technology – Security Techniques – Network Security (www.sabs.co.za)

[11] SANS 31000: Risk Management (www.sabs.co.za)