SACSF/G4.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 4.0: Cyber security event and incident reporting

Introduction

South Australian (SA) Government agencies, and suppliers and non-government personnel providing services to SA Government, are responsible to report, manage and respond to cyber security incidents. This capability should be developed in alignment with the South Australian Cyber Security Framework (SACSF), South Australian Protective Security Framework (SAPSF), and Premier and Cabinet Circular PC042 Cyber Security Incident Management.

The SACSF has been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government agencies.

Applicability

This guideline applies to:

- all SA Government agencies and personnel operating on behalf of the agencies; and
- non-government suppliers and personnel that access SA Government information and resources.

The SACSF policy statement that is in line with this guideline is:

- *SACSF Policy Statement 2.2: Incident Management*
  Cyber security incident response plans must be in place and aligned with an overarching incident management process to enable a consistent approach to the management of cyber security incidents. Agencies must report to the Office for Cyber Security in line with the requirements of PC042 – Cyber Security Incident Management.

Scope

These guidelines have been developed to assist agencies and applicable suppliers to understand their event and incident reporting requirements, describe the role of the Department of the Premier

and Cabinet (DPC) as the Control Agency for Cyber Crisis, and provide an overview of the process associated with the incident reporting scheme.

Expectations

Agencies and associated service providers are expected to implement and maintain security incident management procedures, in line with SAPSF and SACSF requirements.

These security incident management procedures are expected to facilitate identification of cyber security events and incidents, which will be reported to the Watch Desk.

Background

The SA Government's ability to deliver services to the community is dependent on the confidentiality, integrity, and availability of a range of ICT systems and assets.

DPC is designated as the Control Agency for Cyber Crisis (the Control Agency) and has the responsibility to take control of the response to cyber related emergencies. This authority for control includes responsibility for tasking and coordination of other organisations in accordance with the needs of the situation.

As per PC042 – Cyber Security Incident Management, all SA Government agencies and applicable suppliers have a requirement to report cyber security events and incidents to the Control Agency for Cyber Crisis.

Cyber security incident reporting assists in the development of a whole of government picture of the threat landscape associated with SA Government ICT assets.

The Watch Desk utilises this understanding to assist in the development of new or updated cyber security advice, capabilities and techniques to better prevent and respond to evolving cyber threats.

Definitions

Events

A cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards, or a previously unknown situation that may be relevant to security.

The identification of a cyber security event does not necessarily mean than an attack attempt or other event has been successful, or that there are any consequences for the security of the SA Government's information or cyber assets. Not all cyber security events will be classified as cyber security incidents. The Watch Desk will make an assessment at the time the event is reported, as to whether it constitutes an incident.

Incidents

A cyber incident is a single or series of unwanted or unexpected event(s) that impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates.

All cyber security incidents that disrupt government systems or services should be reported even if the impact is minimal. This includes:

- an unexplained outage (e.g. system become unavailable or not working as expected)
- a compromise to SA Government information (e.g. data or privacy breach)
- cyber incidents affecting critical infrastructure and essential services providers.

Examples of cyber security incidents may include:

- suspicious system and network activities
- compromise of sensitive or classified data
- unauthorised access or attempts to access a system
- emails with suspicious attachments or links
- denial-of-service attacks
- ransomware attacks
- suspected tampering of electronic devices.

Roles and responsibilities

Control Agency for Cyber Crisis

Following notification of a cyber security event or incident, an assessment will be performed by the Control Agency, in consultation with the reporting agency or supplier, on whether the event constitutes an incident.

Where an event is determined to constitute a cyber security incident, then an additional level of action will be taken by the reporting agency or supplier in line with their existing incident management procedures and will be supported by the Control Agency.

The Control Agency has responsibility to take control of the response to emergencies of a specific type. Personnel from the Control Agency may contact agency and/or supplier staff for follow-up investigative and remedial concerns.

SA Government agencies

In accordance with PC042 – Cyber Security Incident Management, agencies should have procedures in place for both the management and reporting of cyber security events and incidents. Cyber security reporting works in parallel with an agency's own internal processes for incident handling and reporting and is not a substitute for internal incident management responsibilities.

Failure of an individual to comply with requirements for reporting, managing and responding to a cyber security incident in coordination with the Control Agency will be considered in contravention of/failure to comply with a lawful and reasonable direction, and thus misconduct. This may be referred to the reporting agency's chief executive, Department of the Premier and Cabinet's Chief

Executive, the Commissioner for Public Sector Employment and/or other relevant bodies for determination of disciplinary action.

Agency chief executives are accountable for ensuring their agency reports incidents to the Control Agency. Cyber security program owners and cyber security program coordinators are expected to oversee the development and management of an agency's reporting process.

Existing agency incident management processes are expected to identify and delegate responsibility for cyber security event and incident reporting. Watch Desk notification of events or potential incidents may be performed by whomever the agency considered appropriate to do so (e.g. Cyber Security Officer, ICT Support Officer, Service Desk staff, etc).

Once an event is deemed to be, or is otherwise considered an incident, there is an expectation that the agencies' Information Technology Security Adviser will support the operation and coordination of the cyber security incident response and associated reporting.

Preparing to respond to cyber security incidents

Agencies can consider the below questions to better prepare for a cyber security incident. This helps agency personnel better position themselves to detect, respond to, and report cyber security incidents to the Watch Desk.

- Have we identified systems and data that are critical to our business operations?
- Do we have business continuity and disaster recovery plans in place?
- Do we have an up-to-date and regularly exercised incident response plan?
- Do we have the ability to detect and report cyber security incidents as they occur?

When to report

Where an agency or supplier has identified a cyber security event, or otherwise suspects a cyber security incident has occurred, a report should be immediately provided to the Control Agency.

The timing of incident reporting is vital to the response to reduce likely consequences. In many cases, immediate reporting may result in incomplete and potentially inaccurate information, however the advantage gained from early action outweighs the risk of inaccurate or incomplete early reporting.

The types of occurrences that should be reported to the Watch Desk include:

- denial of service (DoS)
- suspicious scanning and reconnaissance activities
- unauthorised access to a network or device
- data exposure, theft or leak
- malicious code / malware
- ransomware
- phishing or spear-phishing.

While the above list does not include all types of events or incidents that should be reported, it can be used as a guide. Not all unwanted or unexpected actions are going to result in the occurrence of a cyber security event or are going to be of interest for reporting or recording purposes.

The types of occurrences that do not require a report to the Watch Desk include:

- non-ongoing malware or virus activity on a standard user device that is easily remediated (e.g. single case of a user device with a virus that is automatically detected and cleaned by existing controls)
- short term outages of non-critical services (e.g. non-business critical machine has an unplanned outage which is easily recovered from within recovery time objectives)
- single cases of standard spam emails without any malicious links or attachments (e.g. marketing or advertisement spam, or scams without any malicious links or attachments)
- normal background activity detected in logs e.g. standard, regular activity seen in log managers or Security Information and Event Management 'SIEM' systems)
- users breaching agency specific policies or guidelines for appropriate usage of government internet (e.g. single user browsing inappropriate, but not illegal or malicious, websites during work time)
- unexploited vulnerability in non-critical information systems, services, or network (e.g. unpatched vulnerabilities of desktop machines which have not been exploited).

How to report

A report may be submitted by whomever the agency considers appropriate to do so, which may be a cyber security officer, ICT support officer or service desk personnel. The agency will ensure that the appointed agency security executive (ASE) or security advisors (ASAs and ITSAs) are informed of the report.

Reports should be made to the contact information below. The Watch Desk will engage with agencies on alternative reporting process, as required.

- Phone: 1300 244 168 – Press 2
- Email watchdesk@sa.gov.au.

What to include in a report

Where possible, the following information should be included in a cyber security incident report to the Watch Desk:

- the date and time the cyber security incident occurred
- the date and time the cyber security incident was discovered
- a description of the cyber security incident
- any actions taken in response to the cyber security incident
- to whom the cyber security incident was reported
- if assistance is required for incident response.

Integrity of evidence

When gathering evidence following any form of cyber security incident, it is important that its integrity is maintained. Even though an investigation may not directly lead to a law enforcement agency prosecution, it is important that the integrity of evidence such as logs, audit trails have maintained integrity.

Post-incident report

Post-incident analysis after a cyber incident can assist in determining whether a malicious actor has been removed from a system.

A further post-incident report provides opportunities to improve technical security measures, response processes, government policy and ensure lessons learned from incidents are included in assurance process. Agencies may be asked to provide information to the Watch Desk for inclusion during a post-incident review.

Additional considerations

Cyber security incidents involving illegal activity should be reported to SA Police (SAPOL) and the Watch Desk.

The Watch Desk is the single point of contact for the Australian Cyber Security Centre (ACSC) regarding cyber security incidents. Agencies do not need to independently report cyber security incidents to the ACSC.

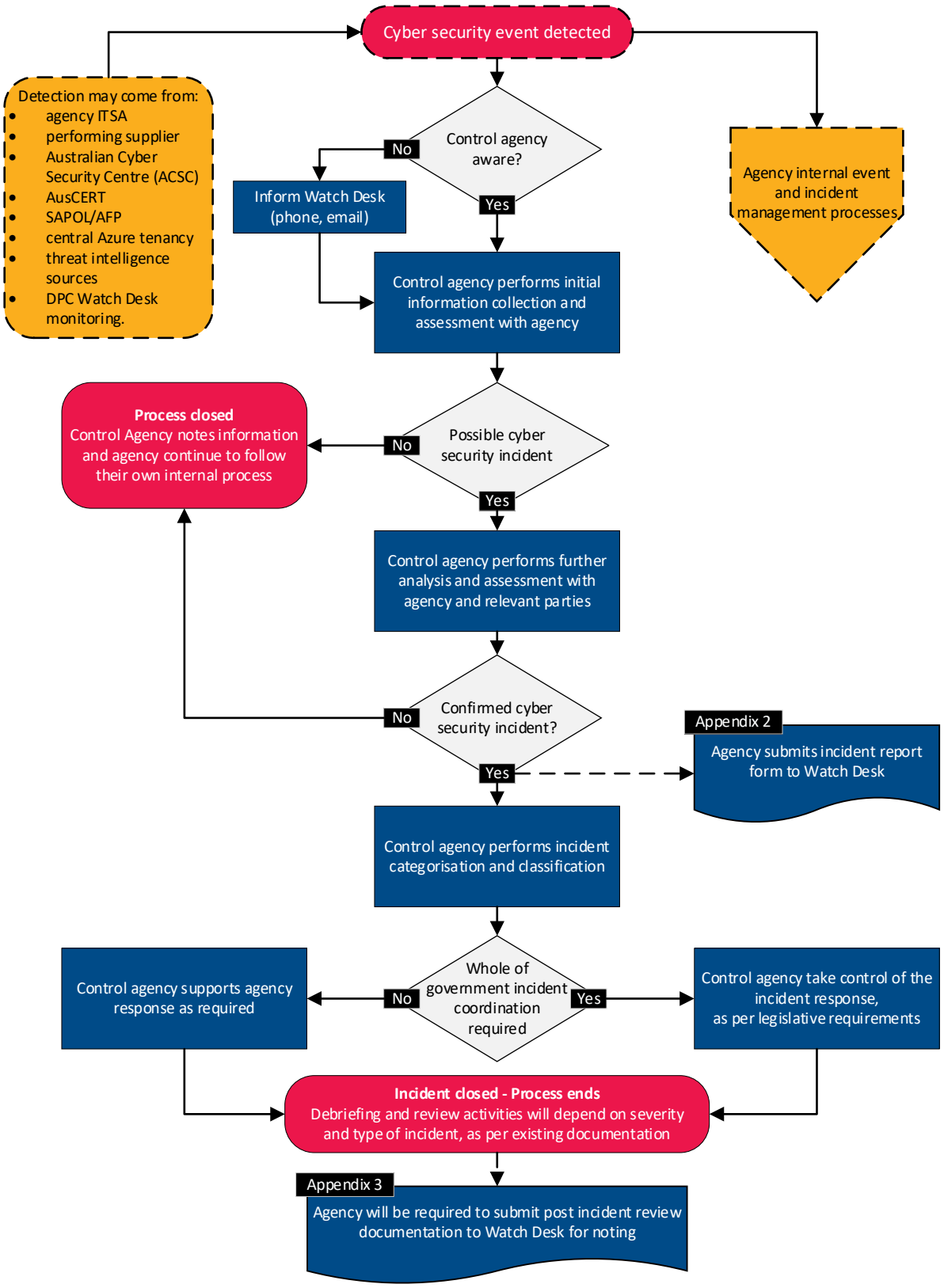

Figure 1 - Cyber security reporting process

References, links and additional information

- South Australian Cyber Security Framework (SACSF)
- South Australian Protective Security Framework (SAPSF) Executive Guide
- PC042 – Cyber Security Incident Management
- PC030 – Protective Security in the Government of South Australia
- Cyber Crisis Incident Management Framework

This guideline does not aim to provide the reader with all of the responsibilities and obligations associated with cyber security incident reporting. It is highly recommended that agencies review all related documents in their entirety. The individual requirements of agencies will have direct bearing on what measures are implemented to mitigate identified risk(s).

Abbreviations

ACSC	Australian Cyber Security Centre
AFP	Australian Federal Police
CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPC	Department of the Premier and Cabinet
ICT	Information Communication Technology
ITSA	Information Technology Security Adviser
PDA	Personal Digital Assistant
SACSF	South Australian Cyber Security Framework
SAPOL	South Australia Police
SAPSF	South Australian Protective Security Framework
SOE	Standard Operating Environment

Document Control

ID	SACSF/G4.0
Version	1.0
Classification/DLM	OFFICIAL
Compliance	Discretionary
Original authorisation date	November 2021
Last approval date	November 2021
Next review date	November 2022

Appendix 1 – Incident Categories

These incident categories are used by the Watch Desk for categorisation and reporting purposes.

Term	Description
Phishing or social engineering	Attempts to acquire information such as usernames, passwords or other sensitive information using social engineering or technical subterfuge.
Spear phishing	Phishing or social engineering attempts that are specifically targeted against an individual or groups. These attempts make use of specific details which are unique to those being targeted to increase their probability of success.
Theft/loss of assets	The theft or loss of any information or technology asset/device (including portable and fixed media) that might have been or has been used to either process or store SA Government information.
Unauthorised access to information/systems	Unauthorised access from internal and external sources to SA Government information and systems.
Unauthorised release of, or disclosure of information	Unauthorised release or disclosure of SA Government information to an unknown environment.
Malware infections	Software programs designed to cause damage to SA Government systems.
Intrusions against networks	Intrusions specifically targeting SA Government internal infrastructure. This includes, but is not limited to: • denial-of-service (DoS)/distributed denial-of-service (DDoS) • website defacements • brute force attempts. Intrusion that cannot be attributed, after analysis, to what is considered consistent with Internet noise. For example, intrusion attempts that consistently target internal network infrastructure, users or services provided for external use such as web applications.
Abuse of privileges	Changes to privilege use settings on stand-alone or networked equipment including network profiles, local user or device configuration files that have not been approved through the agency's change management process.

Term	Description
Unauthorised changes to information, applications, systems or hardware	Any unauthorised changes to an organisation's file system, including media, through insertion, modification or deletion: e.g. changes to standard operating environments (SOEs), addition of executables or the modification of an executable's configuration. Any unauthorised installation of additional processing, communications or storage equipment into the IT network. This includes, but is not limited to: modems, portable games units, smart phones, PDAs or wireless access points.
Violation of information security policy	Any violation of information security policy or the information security related aspects of the code of conduct.
Suspicious system behaviour or failure (hardware/software) or communications)	Unknown network activities affecting/degrading network performance with increased network bandwidth usage and decreased response time, using excessive CPU, increased suspicious network requests or increased Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) alerts leading to application crashes. Includes a malfunction within the electronic circuits, electromechanical components of a computer/communications system, or malfunction/inability of a program to continue processing due to erroneous logic.
Password confidentiality	Sharing/stealing/loss of passwords or other authentication token.
Sabotage/physical damage	Any damage or destruction of physical information or electronic devices.
Other events	Natural events and other events which result in damage to information and systems. This includes but is not limited to fire and flood.