SACSF/G4.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 4.0 – Cyber security event and incident reporting

Purpose

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

Scope

This guideline applies to:

- South Australian Government public sector agencies, that is, administrative units, bodies corporate, statutory authorities and instrumentalities of the Crown as defined in the *Public Sector Act 2009*.
- Suppliers to the SA Government and non-government personnel providing services to agencies.

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 Cyber Security in OCIO in line with the requirements of PC042 – Cyber Security Incident Management.

Guideline detail

These guidelines have been developed to assist agencies and applicable suppliers to understand their event and incident reporting obligations, describe the role of the Department of the Premier and Cabinet (DPC) 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 SA Government Cyber Security Watch Desk (Watch Desk) within DPC as the Control Agency for Cyber Crisis.

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. Cyber security incident reporting assists in the development of a whole of government picture of the threat landscape associated with SA Government ICT assets. All SA Government agencies and applicable suppliers have a requirement to report cyber security events and incidents to the Watch Desk.

DPC is designated as the Control Agency for Cyber Crisis[1] (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.

The Watch Desk uses cyber security incident reports as the basis for helping agencies. Cyber security incident reports are also used by the Watch Desk to identify trends and maintain an accurate threat environment picture.

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. Agencies are required to internally coordinate their reporting of cyber security incidents to the Watch Desk under PC042 – Cyber Security Incident Management.

Definitions

Cyber Security 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.

Cyber Security Incidents

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

Cyber security incidents can be caused by a range of threat actors, including cyber criminals, state-sponsored actors, political 'hacktivists', insider threats and online vandals.

[1] 1.1 – Premier and Cabinet Circular PC042

They can significantly disrupt the delivery of critical infrastructure and essential services, as well as causing:

- disclosure and loss of personal information
- loss of economic, business or employment opportunities
- impact on emotional and psychological wellbeing of affected persons.

The outcomes of cyber incidents can have significant and long-lasting consequences for government, industry and the community.

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[2]. 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 must have procedures in place for both the management and reporting of cyber security events and incidents[3]. 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[4].

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, DPC's Chief Executive, the Commissioner for Public Sector Employment and/or other relevant bodies for determination of disciplinary action.[5]

Agency chief executives are accountable for ensuring their agency reports incidents to the Watch Desk. Cyber security program owners and cyber security program coordinators are expected to oversee the development and management of an agency's reporting process.[6]

Once an event is deemed to be, or is otherwise considered an incident, there is an expectation that the agencies' Information Technology Security Advisor[7] will support the operation and coordination of the cyber security incident response and associated reporting.

[2] 1.2 – Premier and Cabinet Circular PC042
[3] 3.2 – Premier and Cabinet Circular PC042
[4] 3.4 – Premier and Cabinet Circular PC042
[5] 4.4 – Premier and Cabinet Circular PC042
[6] 4.1 – Premier and Cabinet Circular PC042

Reporting cyber security events and incidents

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 Watch Desk.

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.

What to report

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

Occcurrence types that should be reported	Description
Data breaches	• Unauthorised access or theft of sensitive information, such as customer data, personal information, financial records, or intellectual property.
Phishing attacks	• Deceptive emails, messages, or websites designed to trick users into revealing sensitive information, such as usernames, passwords, or credit card details.
Social engineering attacks	• Manipulation of individuals or employees through psychological manipulation to disclose sensitive information, perform certain actions, or gain unauthorised access to systems.
Insider threats	• Malicious activities or data breaches initiated by employees or trusted individuals within an organisation, either intentionally or unintentionally.
Malware infections	• Installation or execution of malicious software, such as viruses, worms, Trojans, or spyware, that can disrupt systems, steal data, or provide unauthorised access.
Advanced Persistent Threats (APTs)	• Sophisticated and prolonged cyber attacks by well-resourced adversaries targeting specific organisations or industries to gain unauthorised access, steal data, or perform espionage.
Credential theft	• Theft or compromise of usernames, passwords, or authentication tokens, leading to unauthorised access to systems or accounts.
Website defacement	• Unauthorised changes made to a website's appearance, often to display political or ideological messages, indicating a breach of security controls.
Supply chain attacks	• Exploitation of vulnerabilities within the supply chain to compromise systems or introduce malicious components into software or hardware.
Mobile device security breaches	• Compromise of smartphones, tablets, or other mobile devices, leading to unauthorised access to personal data, location tracking, or financial fraud.
Internet of Things (IoT) attacks	• Compromising IoT devices, such as smart home appliances, medical devices, or industrial control systems, to gain unauthorised access, disrupt operations, or conduct surveillance.

Data exfiltration	• Unauthorised extraction or theft of data from an organisation's network, often involving sensitive or proprietary information.
Ransomware attacks	• Infection of systems with malicious software that encrypts data, making it inaccessible to the user. Attackers demand a ransom payment in exchange for the decryption key.
Distributed Denial-of-Service (DDoS) attacks	• Coordinated efforts to overwhelm a network, server, or website with a flood of traffic, rendering it inaccessible to legitimate users.
Cyber espionage	• The unauthorised access, theft, or surveillance of sensitive information or intellectual property for strategic, political, or economic gain.
Business Email Compromise (BEC)	• A type of phishing attack where attackers impersonate executives or trusted individuals to deceive employees into transferring funds or disclosing sensitive information.
Cryptojacking	• Unauthorised use of a victim's computer or device to mine cryptocurrencies without their knowledge or consent.
Zero-day exploits	• Exploitation of software vulnerabilities that are unknown to the software vendor, leaving systems exposed to attacks until a patch or fix is released.
Insider trading breaches	• Unauthorised access or use of confidential information by insiders, such as employees or contractors.

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 occurrences are recommended for reporting purposes.

The types of occurrences that are **not recommended** to report to the Watch Desk include:

Occcurrence types that do not need to be reported	Description
Non-critical service outages	• Short-term outages of non-critical services that can be quickly recovered from within recovery time objectives. For instance, a non-business critical machine experiencing an unplanned outage that can be resolved promptly.
Single spam emails	• Single cases of standard spam emails without any malicious links or attachments. This includes marketing or advertisement spam or scams without any harmful elements.
Normal background log activity	• Normal background activity detected in logs, such as regular and expected activities observed in log managers or Security Information and Event Management (SIEM) systems.
Agency-specific policy breaches	• Instances of users breaching agency-specific policies or guidelines for appropriate usage of government internet. This pertains to a single user browsing inappropriate but non-illegal or malicious websites during work time.
Unexploited vulnerabilities in non-critical systems	• Unexploited vulnerabilities in non-critical information systems, services, or networks. This refers to unpatched vulnerabilities in desktop machines that have not been exploited.

What to include in a report

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.

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 or service desk personnel. The agency should 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 methods as required.

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

Methods of Reporting

The following reporting methods offer different channels and mechanisms for individuals to report cyber incidents to the Watch Desk enabling effective communication and prompt incident response.

Reporting Method	Description
Phone Reporting	• Reporting cyber incidents through phone calls, allowing for immediate communication and the opportunity to provide additional context.
Email Reporting	• Reporting cyber incidents via email, where individuals or organisations can send detailed incident reports to designated recipients.
Incident Reporting Templates	• Using predefined incident reporting templates or forms to ensure consistent and standardised reporting of cyber incidents.
Machine-to-Machine (M2M) Reporting	• Automated reporting of cyber incidents between interconnected systems or devices, allowing for real-time communication and incident sharing.
Security Information and Event Management (SIEM) Integration	• Leveraging SIEM systems to automatically collect and analyse security event logs, generating reports on detected cyber incidents.
Threat Intelligence Platforms	• Reporting cyber incidents through threat intelligence platforms, which enable the sharing of incident data and collaboration with other organisations.

Reporting Considerations

- 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 **except** when *Security of Critical Infrastructure Act 2018* requirements for reporting cyber security incidents exist.
  - SA Police (SAPOL) Cybercrime Investigation Branch
  - Australian Federal Police (AFP) Cybercrime Operations
  - Australian Department of Home Affairs - Cyber and Infrastructure Security.

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 evidence such as manual logs, automatic audit trails and intrusion detection tools have maintained integrity.

Post incident review

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 required to participate and provide information to the Watch Desk for inclusion during a post incident review.

Figure 1 *Cyber security reporting process workflow* provides an overview of the reporting process.

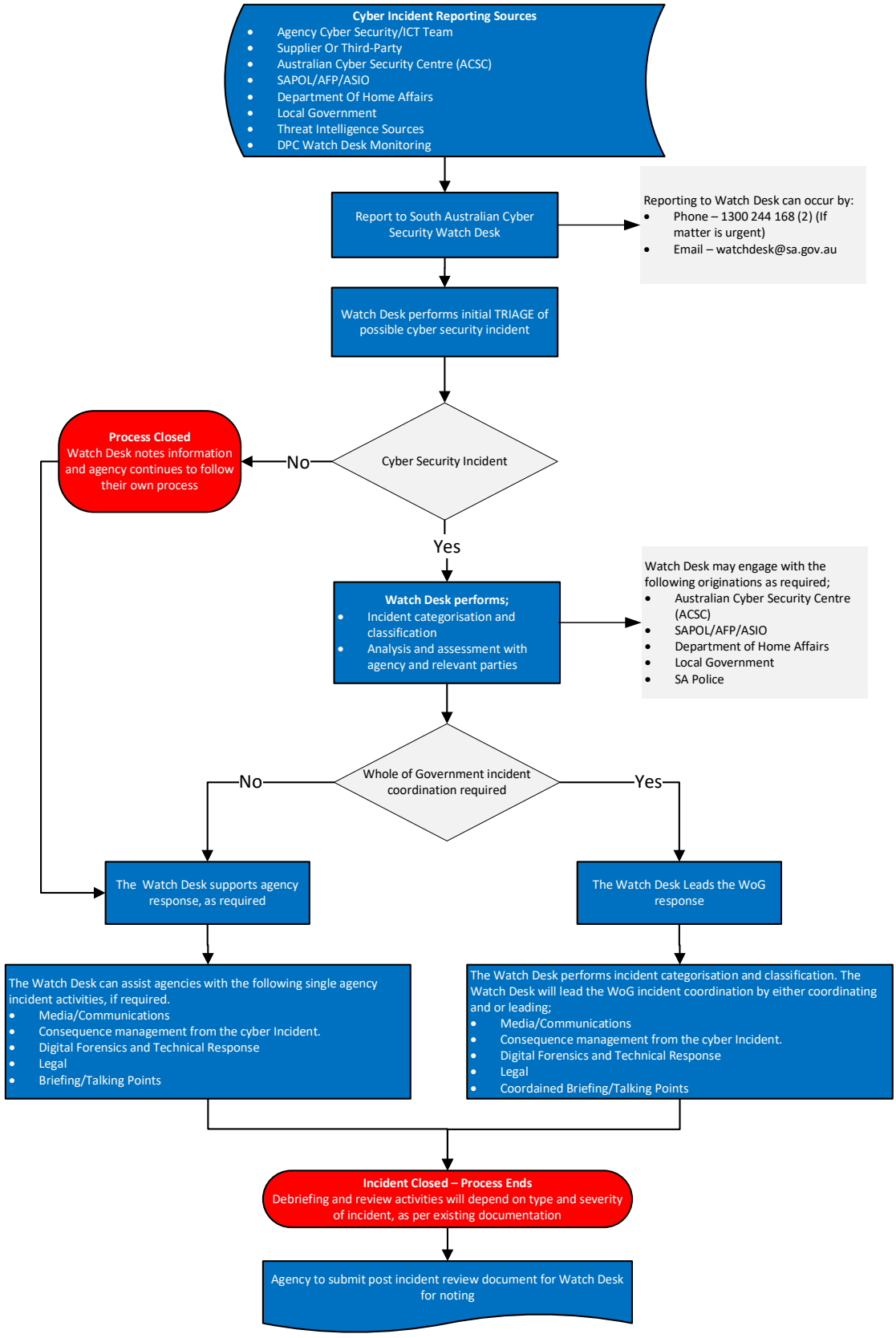

Figure 1 - Cyber security reporting process

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this guideline. There is no specific impact on Aboriginal people.

Related documents

- South Australian Cyber Security Framework (SACSF)
- PC042 – Cyber Security Incident Management
- Cyber Crisis Emergency Management
- Cyber Crisis Incident Management Framework
- South Australian Protective Security Framework (SAPSF)
- South Australian Information Privacy Principles

Acronyms

Acronym	Words
ACSC	Australian Cyber Security Centre
AFP	Australian Federal Police
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPC	Department of the Premier and Cabinet
ICT	Information Communication Technology
ITSA	Information Technology Security Advisor
SACSF	South Australian Cyber Security Framework
SAPOL	South Australia Police
SAPSF	South Australian Protective Security Framework

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Optional
Review number: V2.0	Original approval: November 2021
Next review date: November 2025	Last approval: November 2023