Australian Government

Voluntary Code of Practice for Cyber Incident Response Providers

November 2025

Table of Contents

Purpose

Shield One, Action Six of the *2023-2030 Australian Cyber Security Strategy* (the Strategy) states the Government will provide business and community leaders with greater confidence when they engage cyber security professionals. This includes co-designing a Voluntary Code of Practice (the Code) for cyber incident response providers which will form the technical advice component of Shield One, Action Six.

This Code has been co-designed by the National Office of Cyber Security (NOCS) and Australian Signals Directorate (ASD) alongside industry to ensure that cyber security firms provide fit-for-purpose services consistent with public expectations that support the Australian economy.

Key terms

Term	Definition
National Cyber Security Coordinator	The National Cyber Security Coordinator (the Coordinator) leads whole-of-Government coordination and consequence management activities in response to significant cyber security incidents, as well as preparedness and prevention activities to help anticipate and mitigate the risk of cyber security incidents. The Coordinator is supported by staff from the National Office of Cyber Security (NOCS) within the Department of Home Affairs.
Australian Signals Directorate	The Australian Signals Directorate (ASD) is the Australian Government's leading cyber security agency and aims to make Australia the most secure place to connect online and to foster national cyber security resilience. ASD's Australian Cyber Security Centre (ACSC) monitors cyber threats targeting Australian interests, and provides advice and information, including through an international network of Computer Emergency Response Teams (CERTs) to help protect Australians. When serious cyber incidents occur, ASD leads the Australian Government technical response to help mitigate the threat and strengthen defences.
Cyber security incident	An unauthorised, unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.
Cyber security incident response provider	Usually either internal specialists or an external organisation that provides direct and timely assistance in the detection, containment, remediation, and prevention of cyber incidents.

Introduction

There are currently no consistent standards for cyber incident response providers in Australia. Businesses and individuals rely on these providers to support and guide them through cyber incident response; however, there are no assurances that they are receiving quality service.

During consultation for the Strategy, industry highlighted issues when engaging incident response providers due to a lack of clarity around expected service quality and professional standards. Businesses and individuals often do not have the expertise to understand whether incident response providers are offering useful services and often rely on uninformed trust. Without access to timely and professional support, cyber incidents can grow in scale and consequence.

ASD's ACSC reports that both the frequency and cost of cyber incidents is increasing. In FY 2024-25, over 42,500 calls were made to the Australian Cyber Security Hotline, an increase of 16% from the previous financial year. At the same time, the average cost of cybercrime for small businesses rose by 14% to $56,600 per report, and by 8% for individuals to $33,000 per report.[i] It is imperative that that the Australian Government takes decisive action to ensure that individuals and businesses can rely on incident response providers and receive quality service. Within the Strategy, the Australian Government has made a commitment to ensuring that the responsibility for managing cyber threats is placed with those most capable of doing so.

As the cyber threat landscape continues to evolve, Australians need to be equipped to prevent and respond effectively to cyber incidents. Access to high quality and consistent incident response providers is critical to ensuring collective cyber resilience uplift now and into the future.

This Code is a proactive step towards achieving this. The Code sets out best practice controls designed to support incident response providers to meet service quality and professional standards and encourages early collaboration and information sharing with ASD's ACSC and the Coordinator. The Code recognises that a client's information that is voluntarily shared with ASD's ACSC and the Coordinator will be handled in accordance with the limited use regulations set out in Division 1A of Part 6 of *the Intelligence Services Act 2001* and Part 4 of *the Cyber Security Act 2024.*

Application

This Code is voluntary and should be adopted by providers specialising in the technical component of cyber incident response only. The Code provides guidance on the service quality and professional standards expected from cyber incident response providers, to ensure they are delivering fit-for-purpose services consistently across the Australian economy. At the same time, the Code's principles-based framework aims to preserve flexibility to encourage adoption by providers operating at varying capacity levels.

To ensure currency with the rapidly evolving threat environment, consideration will be given to expanding the scope of the Code in future iterations.

Guiding Principles

1. Identify threats with speed and precision

This principle underscores the importance of using appropriate tools, techniques, and processes to quickly recognise and understand threats once an incident has been identified, and the incident response provider has been engaged. The focus is on identifying the scope, nature, and impact of the threat during the response phase – not on continuous monitoring or pre-incident detection.

By identifying threats with speed and precision during an incident, the provider can help reduce the attacker's window of opportunity, support containment, and enable effective recovery.

The incident response provider should assist their client by:

a. Applying technical and operational expertise to assess the cyber security impacts of the incident.

b. Using structured frameworks, recognising and communicate threat actor tactics, techniques and procedures (TTPs) relevant to the current incident, including those observed in similar cases.

c. Leveraging contextual threat intelligence to enrich understanding of the incident and inform response actions.

2. Investigate to enable recovery and future analysis

This principle recognises that during an incident, the priority is to understand the situation sufficiently to contain the threat and support the organisation's recovery.

While deep forensic analysis may not be feasible or appropriate during active response, if possible, incident responders should collect and preserve relevant information to enable further investigation by specialised teams at a later stage.

By investigating with appropriate depth and context, responders can support informed decision-making, enable rapid recovery, and ensure that artefacts are available for post-incident analysis to strengthen broader cyber resilience.

The incident response provider should assist their client by:

a. Rapidly assessing the incident to understand its scope, impact, and immediate containment needs.

b. Pivoting effectively as new information emerges and adapting response strategies to evolving circumstances.

c. Without interrupting business restoration, collecting and evidentially preserving relevant artefacts (e.g. logs, memory dumps, indicators of compromise) to support future forensic analysis by authorised bodies, including potential sharing with ASD to inform greater insights into the incident and broader cyber defence efforts.[ii] [iii]

d. Providing on-site and remote support as needed to facilitate containment and recovery.

e. Ensuring that investigative actions respect legal boundaries and data handling requirements.

3. Contain the threat while supporting business continuity

This principle recognises that effective containment is essential to limit the spread and impact of a cyber incident. While minimising business disruption is a goal, it may not always be fully achievable during critical containment phases. Incident responders should work with the client to balance operational needs with the urgency of isolating the threat.

At the same time, responders should preserve relevant artefacts during containment (if possible) to support forensic analysis at a later stage.

The incident response provider should assist their client by:

a. Rapidly identifying which systems, networks, or environments require containment based on the evolving understanding of the incident.

b. Advising on tailored containment strategies that consider the client's operation priorities and risk tolerance.

c. If possible, preserving key artefacts (e.g. logs, volatile memory, system images) during containment to support future forensic or regulatory investigations, including potential sharing with ASD's ACSC or other authorised bodies.

d. Supporting the client to identify the likely method of initial access or compromise, where feasible, to inform containment and recovery planning.

4. Remove the threat actor's presence from the system

This principle focuses on identifying and removing the threat actor's access persistence mechanisms, and malicious artefacts from the affected organisation's systems. The goal is to neutralise the threat within the client's environment.

Incident responders should support the client in restoring systems to a trusted state and if possible preserving artefacts that may inform further analysis or government-led operations.

The incident response provider should assist their client by:

a. Where possible, identifying and removing known malicious artefacts and persistence mechanisms from the client's systems.

b. Advising on remediation steps to prevent re-entry or reactivation of the threat actor's access.

c. Supporting system cleansing and reimaging to restore operational integrity.

d. Where possible, preserving relevant artefacts and indicators that may assist ASD or other authorised bodies in broader threat analysis or defensive operations, contributing to the protection of the Australian economy.

e. Validating threat removal through follow-up activities, ensuring the environment is stable and secure before full restoration.

5. Support restoration with actionable insights

This principle recognises that restoring operations is a critical goal following containment and threat removal. While the actual restoration of systems may be undertaken by other service providers, incident responders play a key role in enabling confident recovery by providing timely, accurate, and actionable information.

By supporting restoration through insights and recommendations, responders help ensure that systems are returned to a trusted state and that resilience is uplifted to prevent future compromise.

The incident response provider should assist their client by:

a. Advising on recovery strategies, risks and providing technical insights that support restoration efforts in alignment to the business criticality of the incident, including tailored recommendations to strengthen cyber posture.

b. Sharing investigation findings that inform tactical remediation, such as preventing reactivation of malware or re-entry by threat actors.

c. Monitoring for signs of reinfection or residual threats during and after the recovery phase, if within scope.

d. Coordination with internal IT teams or third-party providers to ensure restoration actions are informed by the incident response findings.

6. Build trust through collaboration

This principle emphasises the importance of open, timely, clear and respectful communication between incident response providers, affected organisations, government agencies, and other stakeholders. Trust is built through transparency, professionalism, and a shared commitment to resolving incidents and strengthening collective cyber resilience.

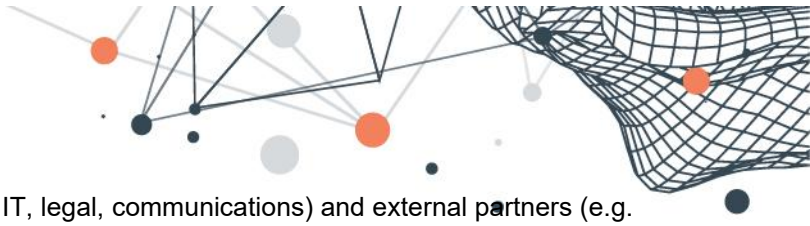
Incident responders should actively collaborate on the technical aspects of the incident, including engaging early with ASD's ACSC and other relevant bodies to support broader national cyber defence efforts. Collaboration must also extend to internal teams, third-party providers, and other entities involved in the response.

This principle underscores the belief that a unified and trusting collective team is better equipped to tackle challenges and drive success.

The incident response provider should assist their client by:

a. Communicating findings and updates clearly and regularly throughout the incident response lifecycle.

b. Engaging early with ASD's ACSC and other relevant government agencies on the technical aspects of the incident, recognising that information shared may assist government to perform its functions in support of the client during an incident.



c. Collaborating with internal stakeholders (e.g. IT, legal, communications) and external partners (e.g. managed service providers, cyber insurers) as needed to support a coordinated response.

d. Recognising the role of government at all levels in managing the broader impacts of cyber incidents.

e. Maintaining confidentiality, integrity, and accountability in all interactions.

7. Support timely and effective reporting

This principle highlights the importance of prompt and accurate reporting during a cyber incident to protect business operations and contribute to broader cyber defence efforts. While the responsibility for formal reporting lies with the affected organisation, incident response providers play a key role in enabling that reporting through timely information sharing and coordination.

Early engagement with relevant government agencies, including ASD's ACSC and the Coordinator, helps ensure that both the organisation and national authorities have the information needed to respond effectively.

The incident response provider should assist their client by:

a. Providing (if requested) clear and actionable reporting that meets the client's internal and external requirements.

b. Engaging early with ASD's ACSC, the Coordinator and other relevant government agencies to support coordinated incident response and national situational awareness.

c. Supplying technical information efficiently to help clients meet their regulatory, legal, and contractual reporting obligations.

8. Turn lessons into defences

This principle encourages a proactive approach to learning from cyber incidents by translating insights into tangible improvements. Incident response providers play a key role in helping organisations understand what happened, why it happened, and how to prevent similar incidents in the future.

While the implementation of long-term changes may be led by internal teams or other partners, incident response providers should support this process by contributing technical insights and strategic recommendations.

The incident response provider should assist their client with the following activities **only within the scope for which they were engaged**:

a. Providing clear technical findings and recommendations to support lessons learned and inform future improvements.

b. Recommending strategic enhancements to security posture, including improvements to tooling, processes, and system architecture.

c. Supporting the client in translating incident insights into practical defences that strengthen resilience against future threats.

d. Sharing de-identified intelligence with government to improve national resilience.

Resources

The following are useful resources that can be shared with clients to help uplift cyber security posture:

a. Cyber Coordinator
b. Cybersecurity Framework | NIST
c. Cyber.gov.au
d. Cyber Security Act
e. Factsheet – Limited Use for the National Cyber Security Coordinator
f. Limited use obligation for the Australian Signals Directorate
g. National Office of Cyber Security Resources
h. FIRST_EthicsfIRST.pdf

---

[i] *Australian Signals Directorate Annual Cyber Threat Report 2024-2025*, Australian Signals Directorate, Canberra, Annual Cyber Threat Report 2024-2025 | Cyber.gov.au.

[ii] *ISO/IEC 27037,* The International Organization for Standardization, ISO/IEC 27037:2012(en), Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

[iii] *Guide to Integrating Forensic Techniques into Incident Response, August 2006*, National Institute of Standards and Technology (NIST), Gaithersburg, NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response