TS 00075.2:1.0

Standard

Cyber Security Incident Management

Part 2: Compliance and Reporting

Issue date: 22 July 2024

Effective date: 22 July 2024

Disclaimer

This document has been prepared by Transport for NSW (TfNSW) specifically for its own use and is also available for use by NSW public transport agencies for transport assets.

Any third parties considering use of this document should obtain their own independent professional advice about the appropriateness of using this document and the accuracy of its contents. TfNSW disclaims all responsibility and liability arising whether directly or indirectly out of or in connection with the contents or use of this document.

TfNSW makes no warranty or representation in relation to the accuracy, currency or adequacy of this document or that the document is fit for purpose.

The inclusion of any third party material in this document, does not represent an endorsement by TfNSW of any third party product or service.

For queries regarding this document, please email Transport for NSW Asset Management Branch at standards@transport.nsw.gov.au or visit www.transport.nsw.gov.au

Document information

Owner:	Director Telecom Engineering Asset Management Safety, Environment and Regulation
Mode:	Multimodal
Discipline:	Security

Document history

Revision	Effective date	Summary of changes
1.0	22/07/2024	First issue

Preface

This document is a first issue.

This document outlines cyber security incident management compliance obligations arising from Australian Government and NSW Government policy, legislation and regulations and mandatory industry standards.

This document sets out processes and specifies procedures to meet these obligations.

The series includes the following documents:

- TS 00075.1 *Cyber Security Incident Management – Part 1: Overview and Principles*
- TS 00075.2 *Cyber Security Incident Management – Part 2: Compliance and Reporting*

Table of contents

1 Scope

This document specifies requirements to meet cyber security incident management compliance obligations arising from Australian and NSW Government policy, legislation and regulations and contractual agreements.

This document sets out reporting requirements to meet the following obligations:

- reporting of cyber security events and incidents to TfNSW from asset stewards
- reporting of cyber security events and incidents from TfNSW to external bodies
- reporting of cyber security events and incidents from agencies or entities to external bodies in certain circumstances
- recording evidence to support attestations and certifications
- recording, use and disclosure of information related to cyber security events and incidents

This standard is based on ISO/IEC 27035.2.

2 Application

This document applies to new and altered assets and may require alterations to existing asset-related processes.

This document applies to asset stewards and service providers who are responsible for technology systems.

3 Referenced documents

The following documents are cited in the text. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

International standards

ISO/IEC 27035.2 *Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*

Legislation

Crimes Act 1900 (NSW)

Data Sharing (Government Sector) Act 2015 (NSW)

Health Records and Information Privacy Act 2002 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW)

Rail Safety National Law (NSW) 2012 (NSW)

Security of Critical Infrastructure Act 2018 (Cth)

State Emergency and Rescue Management Act 1989 (NSW)

State Records Act 1998 (NSW)

Telecommunications Act 1997 (Cth)

Other referenced documents

Department of Customer Service, *NSW Cyber Incident Response Plan*

Department of Customer Service, *NSW Cyber Security Policy*

Department of Customer Service, *NSW Government Information Classification, Labelling and Handling Guidelines*

Premier's Department, *NSW Cyber Security Incident Emergency Sub Plan – A Sub Plan of the State Emergency Management Plan*

Premier's Department, *State Emergency Management Plan (EMPLAN)*

TfNSW, CPr22003.1 *Privacy Data Breach Response Procedure* (This document is not publicly available. To obtain access email standards@transport.nsw.gov.au)

TfNSW, CPSt22005 *Transport Cyber Security Incident Management Standard* (This document is not publicly available. To obtain access email standards@transport.nsw.gov.au)

TfNSW, CPSt23014 *Transport Payment Card Data Security Standard* (This document is not publicly available. To obtain access email standards@transport.nsw.gov.au)

4 Terms, definitions and abbreviations

The following terms, definitions and abbreviations apply in this document.

asset steward the party given the responsibility by a custodian to oversee part of the life cycle process for an asset

cybercrime crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It includes crimes where computers facilitate an existing offence, such as online fraud or online child sex offences. (Source: *NSW Cyber Security Policy*)

information security event occurrence indicating a possible breach of information security or failure of controls. (Source: ISO/IEC 27035-1 ed. 2.0 Copyright © 2023 IEC Geneva, Switzerland. www.iec.ch)

information security incident one or multiple related and identified information security events that can harm an organisation's assets or compromise its operations. (Source: ISO/IEC 27035-1 ed. 2.0 Copyright © 2023 IEC Geneva, Switzerland. www.iec.ch)

security event occurrence in a system that is relevant to the security of the system. (Source IEC TS 62443-1-1 ed. 1.0 Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

security incident adverse event in a system or network, or the threat of the occurrence of such an event. (Source: IEC TS 62443-1-1 ed. 1.0 Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

TfNSW Transport for NSW

5 Legal and regulatory compliance requirements

Cyber security incidents are subject to a range of legislation which includes the following:

- *Crimes Act 1900*
- *Data Sharing (Government Sector) Act 2015*
- *Health Records and Information Privacy Act 2002*
- *Privacy and Personal Information Protection Act 1998*
- *Rail Safety National Law (NSW) 2012*
- *Security of Critical Infrastructure Act 2018*
- *State Emergency and Rescue Management Act 1989*
- *State Records Act 1998*
- *Telecommunications Act 1997*

Cyber security incident management shall comply with the following NSW Government policies and plans:

- *NSW Cyber Security Policy*
- *State Emergency Management Plan (EMPLAN)*
- *NSW Cyber Security Incident Emergency Sub Plan – A Sub Plan of the State Emergency Management Plan*
- *NSW Cyber Incident Response Plan*
- *NSW Government Information Classification, Labelling and Handling Guidelines*

6 Cyber security incident reporting

Asset stewards shall assess and report cyber security incidents in accordance with Section 6.1.

Asset stewards shall implement a procedure for the notification and reporting of cyber security incidents within their service providers.

Note: In the context of a service provider, notifiable and reportable cyber security incidents include those which relate to the assets and services that the service provider provides to the asset steward and those within the service providers organisation.

6.1 Asset stewards reporting to TfNSW

Asset stewards shall notify the TfNSW area responsible for group cyber security of a cyber security incident immediately, but no later than within four hours, when they become aware of, or suspect that, a cyber security incident has occurred, is occurring or is imminent.

If the cyber security incident concerns personal information asset stewards shall also notify the TfNSW area responsible for legal and privacy in accordance with CPr22003.1.

Agencies shall report cyber security incidents to TfNSW in accordance with the *NSW Cyber Security Policy*. Asset stewards shall notify TfNSW by submitting a report using one or more of the following methods:

- online using MyTransport on the TfNSW internal portal
- by emailing transportnsw@service-now.com
- by phoning 133 148.

Note: The TfNSW internal portal may not be accessible to external entities.

Reports shall include the information specified in Appendix A to the extent known after making reasonable inquiries.

6.2 TfNSW reporting to external bodies

The TfNSW area responsible for group cyber security shall coordinate all necessary notification and reporting to external bodies, except where an agency or entity has a specific regulatory obligation to do so, including but not limited to the following:

- Cyber Security NSW
- Australian Cyber Security Centre (ACSC)
- NSW Police Force
- State Emergency Operations Centre (SEOC)
- other affected agencies.

If the cyber security incident also involves a payment card information breach additional notification and reporting obligations to affected parties apply. Refer to CPSt23014.

If the cyber security incident also involves a data or privacy breach additional notification and reporting obligations to affected parties apply. Refer to CPr22003.1.

If the cyber security incident is considered or initially assessed as criminal, it is to be reported in accordance with the *NSW Cyber Incident Response Plan*.

The TfNSW area responsible for group for cyber security shall follow CPSt22005 for cyber incident severity classification, reporting requirements and time frames to external bodies.

6.3 Agency or entity reporting to external bodies

In addition to reporting to TfNSW, agencies or entities shall directly notify and report cyber security incidents to external bodies only where they have a specific regulatory obligation to do so.

For example, under the *Rail Safety National Law (NSW) 2012* rail transport operators are required to report to the Office of the National Rail Safety Regulator (ONRSR) all notifiable occurrences that occur on, or in relation to, their railway premises or railway operations.

Appendix A Cyber security event and incident reporting records (normative)

A.1 Cyber security event reports

Reports shall include the following information to the extent known after making reasonable inquiries:

- date of event
- event number and any applicable related event/or incident numbers
- contact details for the person making the report
- event description and details:
    - what, why or how it occurred
    - initial assessment of assets possibly affected and business impact
    - any vulnerability identified
- date and time the event
    - occurred
    - was discovered.
    - was reported.

A.2 Cyber security incident reports

Reports shall include the following information to the extent known after making reasonable inquiries:

- contact details for the person making the report
- organisational details for the party making the report
- incident classification
- incident details:
    - date and time the incident was identified and whether it is ongoing
    - whether the incident is impacting information technology, operational technology, or customer data
    - nature or type of incident
    - how the incident was discovered

- any other relevant information
- whether the cyber security incident also involves a payment card information breach
- whether the cyber security incident also involves a data or privacy breach
- whether the cyber security incident is also assessed as a cybercrime.