

How to Report a Cyber Incident (Blueprint)

Cyber Incident Reporting Briefing Note for Higher Education
Provider Senior Leadership



Enhancing Cyber Security
Across Australia's Higher Education Sector

WHAT IS A CYBER INCIDENT?

Note: The Australian higher education sector is deemed critical infrastructure and as such specific Government direction regarding the reporting of cyber security incidents may apply for some higher education providers. In particular, it may be relevant to large higher education providers, especially those with links to the defence industry, or those who are involved in significant research activities.

Cyber Security Incidents

Cyber security incidents occur when security measures fail or when an organisation's systems or data are breached – this includes any occurrence that jeopardises the confidentiality, integrity and availability of data or constitutes a violation or threat of violation of a law, security policy or procedure. Perimeter breaches and external attacks, as well as insider threats and incompetence, are all possible causes of security events.

According to the Australian Cyber Security Centre (ACSC), a cyber security incident is defined as one or more acts, events, or circumstances involving:

- unauthorised access to or modification of computer data or computer program; or
- unauthorised impairment of electronic communications to or from a computer; or
- unauthorised impairment of the availability, reliability, security or operation of computer data, a computer program or a computer.

Critical Infrastructure

The ACSC defines Critical Infrastructure as:

"Physical facilities, supply chains, information technologies and communication networks which if destroyed, degraded or rendered unavailable for an extended period would significantly impact on the social or economic wellbeing of the nation, or affect a nation's ability to conduct national defence and ensure national security."

The *Security Legislation Amendment (Critical Infrastructure) Act 2021* covers eleven critical infrastructure sectors, including higher education and research. The Act modified and broadened the definition of critical infrastructure to safeguard the sector promptly in the event of a significant cyber attack. This capability established higher education duties such as having a register of critical higher education assets, responding to requests for information, directives for action, or requested involvement in response to major cyber security events affecting a 'critical education asset.'

HOW TO REPORT A CYBER INCIDENT

There are a number of options that higher education providers have to report cyber security incidents, these include the following.

ReportCyber

[ReportCyber](#) is the online reporting mechanism through which individuals and businesses (both small and large) can report cyber crimes.

Cyber crime is the use of a computer or online network to commit crimes such as fraud, online image abuse, identity theft or threats and intimidation. As cyber crime becomes more sophisticated, criminals are targeting individuals, businesses, education institutions and governments.

Note: ReportCyber should **not** be used when:

- There is already a court order against the suspect
- A physical crime has been committed, such as the person's debit or credit card or computer has been stolen
- The person has received a scam call and no loss of personal information or money has occurred.

Instead, review the ACSC [Report and Recover page](#) to see what other options are available.

Making a Report

Click on this [ReportCyber link](#) to see what is involved in making a cyber incident report to the ACSC/police on behalf of:

1. An individual
2. A small or medium business
3. An organisation or critical infrastructure organisation
4. A Government department or agency.



Best practice reporting

In alignment with critical infrastructure requirements, best practice entails reporting major cyber security incidents within a specific timeframe:

- **12 hours**, if the incident has a significant impact on the availability of the asset, or
- **72 hours**, if the incident has an impact on the availability, integrity or reliability of the asset, or on the confidentiality of information about, or held by the asset.

After the Report is Made

Once the report has been made it will be referred to the appropriate police jurisdiction for assessment. Some cyber crime may constitute an offence under Commonwealth and/or state and territory legislation.

The ACSC will be unable to advise on the progress of a report as it will be referred directly to police for assessment.

If a person has an existing cyber crime report they can check the status of the ReportCyber report.

Note:

- Not all matters will be investigated by law enforcement. However, each report assists to disrupt cyber crime operations and make Australia a secure place to connect online.
- If the person does not report anonymously then they will receive a receipt email confirming their submission and the report number.

Resources

For more information on cybercrime and cyber incident reporting, refer to the following resources:

- The Victorian Government's information on [how to report cybercrime and online scams](#)
- The Australian Cyber Security Centre's information on [reporting a cybercrime, incident or vulnerability](#)
- [Cyber and Infrastructure Security Centre](#) (CISC) information on critical infrastructure, legislation, regulation and compliance.

Sources

This blueprint has been developed using [Cyber and Infrastructure Security Centre](#), [Australian Cyber Security Centre](#), and [Australian Federal Register of Legislation](#) resources.