Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Principles of operational technology cyber security

Quick reference guide

Critical infrastructure is essential to maintaining and enhancing our way of life. Operational Technology (OT) within our critical infrastructure exercises control over many essential services such as the water we drink, the energy we rely on, and the transport that moves us all. Internationally, malicious cyber activity against OT assets is reportedly on the rise.

The principles of OT cyber security are designed to assist decision makers at all levels to give appropriate weight to cyber security risks and best secure the systems that keep our nation running. If a proposal is likely to impact or break one or more of the principles of OT cyber security, then the proposal will likely introduce a vulnerability to the OT environment.

Principle 1: Safety is paramount – ***Ensure the system is safe!***
Safety is critical in physical environments. This includes safety of human life, safety of plant, equipment and the environment, and reliability and uptime of the process. Cyber security controls must be safe, and safety must be informed by the cyber threat environment.

Principle 2: Knowledge of the business is crucial – ***Know and defend vital systems.***
Knowing the business, knowing how processes work, knowing where connections are and what parts are critical, will help an organisation design and implement the most effective cyber security controls and response capabilities for the resources available. Organisations should be able to identify vital systems and have in place an architecture that defends them, and include a restoration and recovery process capable of meeting required business outcomes.

Principle 3: OT data is extremely valuable and needs to be protected – ***Protect OT data.***
For a malicious cyber actor, knowing how a system is set up, how the network is architected, how the controllers are configured, what vendors and devices are used, with which protocols, is like a treasure map for how to cause harm. Put processes in place to minimise access to and distribution of OT data, while ensuring integrity of the OT data.

Principle 4: Segment and segregate OT from all other networks – ***Keep the back door shut.***
Segment and segregate OT from all other networks, including peers, IT and the internet. Consider especially administrative and management role assignments in OT environments.

Principle 5: The supply chain must be secure – ***Secure the cyber supply chain.***
Supply chain security goes beyond software and devices from major vendors. Consider all software, devices and managed service providers in OT, including their support, management and maintenance, from purchasing and integration through to decommissioning and disposal.

Principle 6: People are essential for OT cyber security – ***People are the first line of defence.***
A cyber-related incident in OT cannot be prevented, defended against, identified, responded to and recovered from in a timely manner without people with the necessary tools and training looking for it, and able to competently respond to it. An investment in staff to create a collaborative team of trained and skilled people with necessary tools, supported by a mature and organisation-wide cyber-security culture, is critical to an organisation's cyber defences.

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

National Cyber Security Centre

a part of GCHQ

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Te Tira Tiaki

Government Communications Security Bureau

National Cyber Security Centre

PART OF THE GCSB

Bundesamt für Sicherheit in der Informationstechnik

National Cyber Security Centre

Ministry of Security and Justice

NISC 内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity

警察庁

National Police Agency

This publication was developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) in collaboration with the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), United Kingdom's National Cyber Security Centre (NCSC-UK), Canadian Centre for Cyber Security (Cyber Centre), New Zealand's National Cyber Security Centre (NCSC-NZ), Germany's Federal Office for Information Security (BSI Germany), the Netherlands' National Cyber Security Centre (NCSC-NL), Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA), and the Republic of Korea's National Intelligence Service (NIS) and NIS' National Cyber Security Center (NCSC).