Cyber Security Principles

These IMT Cyber Security Principles outline the responsibilities and online behaviour expectations of all CSIRO employees and affiliates to ensure our people, data and science are protected.

Core Principles

1. Effective cyber security risk management enables CSIRO to achieve its objectives
2. Cyber security is everyone's responsibility
3. Cyber security threats are identified and treated proportionately to protect CSIRO's most valuable assets
4. Cyber security is ongoing

Context

The Cyber Security Principles support the CSIRO Risk Policy to enable cyber security risks to be effectively managed within the organisation. These principles set out the expectations of all CSIRO staff and affiliates in relation to their behaviours towards cyber security.

Principle 1: Effective cyber security risk management enables CSIRO to achieve its objectives

1.1 Security supporting challenges and missions.

- Safety: Cyber security measures enable CSIRO to push the boundaries of research and innovation in a safe and secure manner.
- Efficiency: Cyber security measures support the efficient and effective delivery of research and innovation services.
- Longevity and trust: A strong cyber security culture allows CSIRO to hold and maintain its reputation and 'trusted advisor' status with the Government, industry and the community.

Accountability

- CSIRO Executives are accountable for ensuring that there is a positive cyber security culture within the organisation and that cyber security risk management is incorporated into organisational strategies and plans.

- CSIRO Leaders are accountable for promoting a positive cyber security culture in their teams, supporting staff to undertake training in relation to cyber security and ensuring that cyber security risk management is incorporated into their plans and delivery of services.
- All CSIRO staff are accountable for following authorised policies and procedures and managing CSIRO information appropriately.

Principle 2: Cyber security is everyone's responsibility

2.1 Everyone is accountable for good cyber security practice

- Use and conduct: All staff and affiliates are responsible for the way in which they use ICT services and must do this in a responsible manner. This includes the use of ICT services provided by CSIRO, its partners and other third-party services.
- Protection of assets: All staff and affiliates are responsible for the protection and care of CSIRO's and its partners' ICT and information assets, in accordance with IMT standards and guidelines
- Meet legislative obligations: All staff and affiliates must ensure they act in accordance with legislative requirements and take steps to ensure CSIRO obligations are met.
- Meet community expectations: All staff and affiliates must take reasonable steps to support CSIRO in meeting community expectations for cyber security in order to maintain its reputation and trusted advisor status.

2.2 CSIRO Leaders are responsible for integrating cyber security into their strategy, planning and execution of projects

- Planning: CSIRO Leaders responsible for projects and initiatives must consider cyber security risks and incorporate cyber security measures and costs into their planning.
- Projects: CSIRO Leaders responsible for projects must incorporate cyber security risk management into their project delivery.
- Resource: CSIRO Leaders must adequately resource and budget for cyber security risks to be managed in line with organisational risk.
- Leadership: CSIRO Leaders should model a positive cyber security culture and actively promote the importance of cyber security measures.

2.3 Service owners are responsible for the management of cyber security risks

- IMT: IMT is responsible for providing safe and secure ICT corporate services for the whole of CSIROand management of the cyber security risks in relation to those services.
- Business Units: Business Units that procure and operate non-CSIRO managed ICT services are responsible for managing the cyber security risks of these services, including on-premise and cloud-based services.
- Cyber Security Services: The IMT Cyber Security Services (CSS) team is responsible for providing whole of CSIRO cyber security risk management advice and support for risk managers and owners.

2.4 CSIRO Executive are accountable for cyber security risk management

- Accountability: CSIRO is accountable for its cyber security to its Minister and the Australian Government.
- Authorities: CSIRO's accountable authority is the Board.
- Risk tolerance: The Board, through the Board Audit and Risk Committee, determines CSIRO's tolerance for cyber security risks and the Chief Information Security Officer (CISO) implements controls, countermeasures and mitigations based on tolerance for risk.

Accountability

- See Accountability section in Principle 1

Principle 3: Cyber security threats are identified and treated proportionately to protect CSIRO's most valuable assets

3.1 CSIRO takes measures to identify threats and manage risks to its people, assets, projects, the organisation, partners and the nation.

- Cyber security is incorporated into wider risk management: CSIRO risk management activities shall incorporate the identification, assessment and treatment of cyber security related risks.
- Threat and risk identification: CSIRO takes appropriate measures to proactively identify cyber security threats and risks to its assets, capabilities and projects.
- Range of impacts: The identification of cyber security risk is to be inclusive of, and consider the impacts to staff, individual projects and initiatives, as well as to CSIRO, partners and collaborators, and external parties.

3.2 CSIRO takes a risk proportionate approach to implementing cyber security treatments and mitigations to protect CSIRO, its partners and the nation.

- Baseline measures (cyber hygiene): Cyber security best practices and hygiene are applied across the range of ICT services at CSIRO.
- Treatment proportionality: Security measures are implemented proportionally to the risk they mitigate. Stronger controls are applied to services and information that operate in higher risk environments.
- Best practices: Cyber security measures should align with best practices as outlined by the Australian Government Information Security Manual and other industry best practices.
- Business outcomes: Security treatments must support the business outcome for CSIRO and the performance of research and innovation.

Accountability

- See Accountability section in Principle 1

Principle 4: Cyber security is ongoing

4.1 Cyber resilience

- System design: CSIRO designs services, plans projects, and delivers services in a way that provides for the identification and detection of, and recovery from, cyber threats and incidents.
- Security testing: CSIRO tests the effectiveness of security measures for the systems and services that CSIRO procures and operates to ensure their overall resiliency.
- Detect and respond: CSIRO takes proactive measures to monitor its ICT capabilities to identify, report and respond to cyber threats in a timely manner.
- Disaster recovery: IMT and CSIRO business units that operate their own infrastructure regularly review and test their disaster recovery planning in order to recover from cyber security incidents in an appropriate manner.
- Business continuity: CSIRO business units regularly review and test their business continuity planning in order to allow for the adaptation to disruptions caused by cyber security incidents.

4.2 Continuous improvement

- Monitor performance CSIRO conducts continuous monitoring of the performance of cyber security controls and measures to ensure they are meeting their intended outcome.
- Vulnerability management: IMT and CSIRO business units take proactive measures to identify and test for weaknesses in infrastructure and services it procures and operates in order to improve its cyber security posture.
- Incremental improvements: CSIRO shall continuously take steps to make incremental improvements to its approach to managing cyber security risks. These in turn have a compounding impact on the broader cyber security capability.
- Effective resourcing: CSIRO shall effectively resource its current cyber security measures and future cyber security initiatives in order to improve its overall cyber security posture.

Accountability

- See Accountability section in Principle 1

Accountability

Authors

Kat Southall

Functional areas included

IMT

Approver

Brendan Dalton

Date of final approval

06 August 2020