Government of South Australia

SACSF/G17.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 17.0: Internet of Things (IoT) Security

Purpose

Cyber security is fundamental to the successful operations of the South Australian Government. The South Australian Cyber Security Framework (SACSF) and supporting guidelines have been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of South Australian Government agencies.

This guideline has been developed to assist agencies to manage the security risks associated with Internet of Things (IoT) technologies, including the risks introduced by the IoT devices, services, and third parties. This guideline should be applied to all IoT device procurement and management processes.

Scope

The SACSF applies to:

- South Australian Government public sector agencies, that is, administrative units, bodies corporate, statutory authorities and instrumentalities of the Crown as defined in the *Public Sector Act 2009*.
- Suppliers to the SA Government and non-government personnel providing services to agencies.

The SACSF policy statements related to this guideline are:

- *SACSF Policy Statement 1.5: Supplier Management* – Cyber security requirements must be included in all agreements with suppliers. Processes for assessing and managing the risks that suppliers introduce must be embedded within the procurement and contract management functions in alignment with the agency's risk management framework.
- *SACSF Policy Statement 2.5: Administrative Access* – Administrative access to agency systems, applications and information must be restricted to personnel with a specific business need which is validated on a periodic basis.

- *SACSF Policy Statement 2.7: Vulnerability Management* – Security vulnerabilities in agency ICT equipment, systems and applications must be identified and managed.
- *SACSF Policy Statement 2.8: Network Communications* – Network communications must be secured, ensuring agency information traversing internal and external networks is appropriately protected based on its classification and can only be accessed by authorised parties.
- *SACSF Policy Statement 4.1: Physical Security* – Protective security must be integrated in the process of planning, selecting, designing and modifying agency facilities for the protection of people, information and physical assets.

Definition

IoT refers to the devices embedded with sensors, software, network communication modules for the purpose of connecting and exchanging data with other devices and systems over the internet.

These devices range from ordinary household objects to commercial, enterprise, or industrial devices, such as smart home appliances, wearable devices, security CCTV cameras, smart buildings, and even smart city systems.

Many IoT devices are the result of the convergence of cloud computing, mobile computing, embedded systems, data analytics, and information processing and networking hardware.

Guidelines

The following cyber security process areas should be considered for procurement and deployment of IoT devices:

- Supplier security risk management
- Authentication and access control
- Vulnerability management
- Secure network communications
- Physical security

The detailed requirements and example implementations are outlined in the following sections.

Process area	Security Principles	Control Implementation
Supplier Security Risk Management	Processes for assessing and documenting cyber security risks that IoT technologies and suppliers may introduce should be embedded within agency's procurement and contract management functions. Security requirements should be defined, and security risks should be identified at the early stage of the procurement and deployment of IoT devices. Security risks should be documented and managed based on the agency's risk appetite, throughout the lifecycle of the device.	**Recommended Controls** • Conduct risk assessments for IoT technologies, services, and vendors to understand the security risks and potential business impacts. Consider: ◦ The classification of information stored or processed by the device. ◦ If the supplier and manufacturer are reputable. ◦ If there are opportunities for the device to be tampered with through the supply chain. ◦ How access to the device is secured, both logical and physical. ◦ How the device is updated to fix vulnerabilities. ◦ How data is securely stored and transmitted. ◦ Data sovereignty and geolocation. ◦ What information is collected by the device, who it is shared with, and how it is used by the supplier (privacy policy). ◦ How personal information is protected. ◦ If the device has any additional functionality which is not required. • Cyber security risk assessment processes should be embedded within procurement and contract management processes for IoT technologies and vendors. • When conducting supplier cyber security risk assessments and assurance activities refer to the Australian Cyber Security Centre IoT Secure-by-Design Guidance for Manufacturers for the security principles that IoT manufacturers should adhere to. • Obtain security assurance from the vendors and their supply chain, that they meet security requirements and expectations, where possible (e.g. ISO 27001 certificate, SOC 2 reports, cyber security related Service Level Agreements). • If the device processes personal information, consider if a Privacy Impact Assessment against the South Australian Information Privacy Principles is required. • If the device stores or processes information offshore, consider the South Australian Protective Security Framework and SACSF Ruling 2 Storage and Processing of Information in Outsourced or Offshore ICT Arrangements requirements.

Process area	Security Principles	Control Implementation
		• IoT devices are often developed with low cost in mind and therefore can lack sophistication to directly implement security controls. In these cases, compensating controls should be considered to reduce the risk to an acceptable level.
		Bad Practices • The security risks from IoT devices are not identified or documented. The business / system owners do not understand the security risks associated with the IoT technology. • IoT devices are deployed without security consideration or controls (shadow IT), impacting the agency's security posture.
Authentication and Access Control	Logical access to the IoT configuration portal, management platform, and connected network devices should be restricted. Passwords of the administrator accounts and services accounts should be complex and long enough to protect the authentication process, with the use of Multi-factor Authentication (MFA) where possible.	**Recommended Controls** • Change the default passwords and set unique, unpredictable, complex, and long passwords for IoT devices and management platforms. • Use a password management solution to manage passwords for IoT devices and related platforms. • Passwords are updated / rotated regularly. • Restrict access to IoT configuration portals, so only authorised personnel have credentials. • Remote access to IoT devices is via secure connections, such as VPNs or jump hosts. • Any supplier or manufacturer remote access is restricted, managed and monitored. • MFA is enabled for IoT devices where possible.
		Bad Practices • Use of factory default passwords on IoT devices. • Access to IoT devices is not configured based on the Need-to-Know principle. • The login credentials, Wi-Fi service set identifier and passwords are shared without authorisation among IoT devices (e.g. IoT devices from the same vendor enable instant setup by sharing credentials to other devices automatically). • IoT device passwords are stored and transmitted in plain text (within configuration files or network packages).
Vulnerability Management	Vulnerabilities in IoT devices should be identified and mitigated. Technical vulnerabilities that are discovered by agencies	**Recommended Controls** • Establish a vulnerability and patching management strategy to address the specific environments and use cases for IoT devices. • Define a procedure for acquiring, testing, and deploying updates to the IoT devices firmware, software, and protocols.

Process area	Security Principles	Control Implementation
	should be notified to suppliers. Patching, updating, and upgrading to the IoT environments should be timely and not impact the devices' functionality, user-configured preferences, security or privacy settings.	• Acquire updates from trusted sources and check the integrity (e.g. checksum) of the update packages. • Isolate or replace IoT devices that are not able to be patched for known vulnerabilities. • Subscribe to the vendor or open-sourced vulnerability disclosure and update notification channels.
		Bad Practices • Use of end-of-life or end-of-support IoT devices without mitigating controls. • Known vulnerabilities are not mitigated in a timely manner.
Secure Network Communications	The network communications of IoT environments should be secured and monitored. Information flows associated with IoT devices should be documented and security assessed based on the classification levels. The IoT web management interface should only be accessible to the local network unless the IoT device needs to be managed remotely via the Internet.	**Recommended Controls** • Document the information flows and perform security assessments for IoT devices and connected networks. • Perform an assessment of the data transmitted over IoT devices and networks, to understand the impact on privacy and critical data within IoT network communications, as well as understanding the impact of denying any traffic flows on the performance of the device. • Segregate the IoT networks from critical systems and corporate networks, and/or deploy IoT devices in isolated network zones. • Monitor network traffic to detect anomalies and malicious network communications in IoT environments. • Disable unused functionality, ports, and logon portals to reduce the attack surface and vectors. • Encryption, as articulated in the *Guidelines for Cryptography*, is used for data in transit and at rest. • Where IoT devices connect to StateNet, the connections must comply with the StateNet Conditions of Connection.
		Bad Practices • Connecting IoT devices to corporate networks or critical security zones without conducting a security architecture review or risk assessment. • The device has multiple unused network ports that are open and listening for connections both before and after device setup. • Bluetooth pairing stays active once the device has been set up despite no longer being used for any device functionality.

Process area	Security Principles	Control Implementation
		• The device exposes unencrypted protocols (e.g. Telnet) which are used to exchange usernames and passwords that gain root access to the device. • The IoT device exchanges data with untrusted network domains and/or Internet service providers. • The IoT network communications are not visible to network monitoring solutions. • The rules of sharing of information and data are not defined for IoT devices and networks.
Physical Security	Physical security controls should be implemented in the process of planning, selecting, and deploying IoT devices to prevent physical damage and unauthorised physical access to the IoT devices and underlying facilities.	**Recommended Controls** • IoT devices and connected facilities are inventoried. • Physical access to IoT devices is restricted to authorised personnel, and access is monitored and logged. • IoT devices are deployed at safe locations, to prevent unauthorised access and environmental damage.
		Bad Practices • IoT devices are located at publicly accessible areas and/or insecure zones without monitoring and physical security controls. • The physical ports and interfaces on the IoT devices are not blocked or disabled, so that anyone can easily reach to and/or connect to them.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this guideline. There is no specific impact on Aboriginal people.

Related documents

List all parent documents including related policies and/or procedures, Acts of Parliament, regulations and other reference or supporting documents. Provide hyperlinks for all.

- South Australian Cyber Security Framework (SACSF)
- South Australian Protective Security Framework (SAPSF)
- ACSC IoT Secure-by-Design Guidance for Manufacturers
- NIST IR 8228 Considerations for Managing IoT Cybersecurity and Privacy Risks
- ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines
- South Australian Information Privacy Principles
- StateNet Conditions of Connection (link available to SA Government employees only)

Acronyms

Acronym	Words
IoT	Internet of Things
CCTV	Closed Circuit Television

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Optional
Review number: V1.0	Original approval: 20 September 2023
Next review date: September 2024	Latest approval: 20 September 2023