Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards

Implementation Guidance for Industrial Automation and Control Systems — Extension to VPDSS Implementation Guidance

Victorian Protective Data Security Standards

Implementation Guidance for Industrial Automation and Control Systems — Extension to VPDSS Implementation Guidance

Document details

Document details	
Protective marking	OFFICIAL
Approved for unlimited public release	Yes
Release date	December 2022
Review date	
Document version	V1.0
Authority	Office of the Victorian Information Commissioner (OVIC)
Author	Information Security Unit – OVIC

Version details

Version	Publish date	Amendments in this version
1.0	December 2022	N/A

Note. The issue of version 1.0 of this document does not represent a change to the Victorian Protective Data Security Standards V2.0. This document has been developed in conjunction with the Victorian Government Industrial Automation and Control Systems (**IACS**) sector.

Victorian Protective Data Security Standards

Implementation Guidance for Industrial Automation and Control Systems — Extension to VPDSS Implementation Guidance

Objectives

The objective of this document is to assist organisations that operate Industrial Automation and Control Systems (**IACS**) with applying the Victorian Protective Data Security Standards (**VPDSS**) to those environments.

This document is intended to be read **in addition** to the *VPDSS Implementation Guidance*[1].

Purpose

The purpose of this document is to identify the differences in implementing the VPDSS for IACS.

Applicability

Part 4, section 84 of the *Privacy and Data Protection Act* 2014 (Vic) (**PDP Act**) defines the VPS organisations that are covered by the VPDSS as well as those that are exempt. This document applies to Part 4 in scope organisations operating IACS.

In practical terms, this includes the water and transport sectors who are a public sector agency or body and may be operating a critical infrastructure asset[2].

Background

IACS operate within a complex environment, often connected directly to physical processes. IACS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical Information Technology (**IT**) environments. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems.

There are some differences between standard enterprise IT and IACS environments that require modification in the approach used to assess and treat cyber security risks. In IACS environments risks will likely vary, with availability and integrity typically of greater focus. There are inherent risks associated with industrial infrastructure and equipment that are controlled, monitored, or otherwise affected by IACS. Security in these systems is primarily concerned with maintaining the availability and integrity of these systems, with confidentiality a significant concern, but relatively less so.

Loss of intellectual property or interruption of the flow of information are not the only consequence of a security incident. Like IT, IACS equipment utilises computer-based technology, which are both susceptible to common cyber security attacks and compromise. However, a cyber security attack or compromise on the IACS could result in devastating real-world consequences to critical infrastructure and availability of services beyond the effected organisation including loss of human life, public safety, and the physical

[1] Available on the OVIC website under Resources https://ovic.vic.gov.au/data-protection/information-security-resources/

[2] For more information on critical infrastructure, refer to the *Security of Critical Infrastructure (**SOCI**) Act* https://www.legislation.gov.au/Details/C2022C00160

environment of the region or the State. Cyber security attacks on both IT and IACS can result in mutual consequences, namely the compromise of information and systems, and significant financial and reputational implications.

Use of specific terms in this document

Please refer to the *VPDSS Glossary* for an outline of terms and associated definitions. For a current copy of the glossary, please refer to the information security resources[3] section of the OVIC website.

In addition, the following terms are relevant and used throughout this document.

Term	Description
Industrial Automation and Control System (**IACS**)	A collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process. These systems include but are not limited to: • industrial control systems, including distributed control systems (**DCSs**), programmable logic controllers (**PLCs**), remote terminal units (**RTUs**), intelligent electronic devices, supervisory control, and data acquisition (**SCADA**), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety-instrumented system (**SIS**) functions, whether they are physically separate or integrated); • associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems; and • associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes. [SOURCE: IEC/TS 62443-1-1 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models]
Reliability, Availability, Maintainability, and Safety (**RAMS**)	The operational objectives of IACS. A decision-making tool to ensure that a process, machinery, or equipment fulfils the mission for which it was designed, under the conditions of reliability, availability, maintainability, and well-defined safety.

[3] Refer to OVIC's website https://ovic.vic.gov.au/information-security/information-security-resources/

Scope

This guidance directs organisations to the International Electrotechnical Commission (**IEC**) 62443 series of standards as the principal primary source for:

- determining systems for inclusion as IACS;
- partitioning of IACS elements into zones[4] and conduits;
- assessing risks relating to each zone and conduit;
- establishing the required security level for each zone and conduit; and
- documenting security requirements.

Structure of this document

This document has been structured in a format similar to the *VPDSS Implementation Guidance V2.1*. All **standards** and **objectives** apply equally to IACS environments, and as such, no changes have been made to these.

In cases where **elements** specified in the *VPDSS Implementation Guidance* are applicable without a need for any additional information, a reference back to the *VPDSS Implementation Guidance* is provided. No additional guidance specific to IACS environments beyond that provided in *VPDSS Implementation Guidance* is required in the following standards:

- Standard 5 – Information Security Obligations;
- Standard 6 – Information Security Incident Management;
- Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery;
- Standard 10 – Personnel Security; and
- Standard 12 – Physical Security.

In cases where **elements** need additional guidance specific to IACS environments, the *VPDSS Implementation Guidance* is applied without modification, as well as the specific IACS guidance related to the standard. IACS sector-specific guidance and information is included in the following standards:

- Standard 1 – Information Security Management Framework;
- Standard 2 – Information Security Value;
- Standard 3 – Information Security Risk Management;
- Standard 4 – Information Access;
- Standard 8 – Third Party Arrangements;
- Standard 9 – Information Security Reporting to OVIC; and
- Standard 11 – Information Communications Technology (**ICT**) Security.

[4] A security zone is a logical grouping of physical, informational, and application assets sharing common security requirements.

Standard 1 – Information Security Management Framework

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 1 applies.

Additional IACS-specific Elements

V2.0 #	Element	Primary Source
E1.120	The organisation's information security management framework defines the relationship between the business areas that support IT security and the business areas that support IACS security.	*IEC TS 62443-1-1:2009 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models* § 5.8.2 Enterprise level policy
E1.130	The organisation's information security management framework differentiates security objectives of the IACS from the enterprise systems.	*IEC TS 62443-1-1* § 5.8.2 Enterprise level policy

IACS-specific implementation guidance

There are two conceptual views commonly used to help with the design of security architectures for organisations to consider. Figure 1 is a reference model highlighting IACS components.

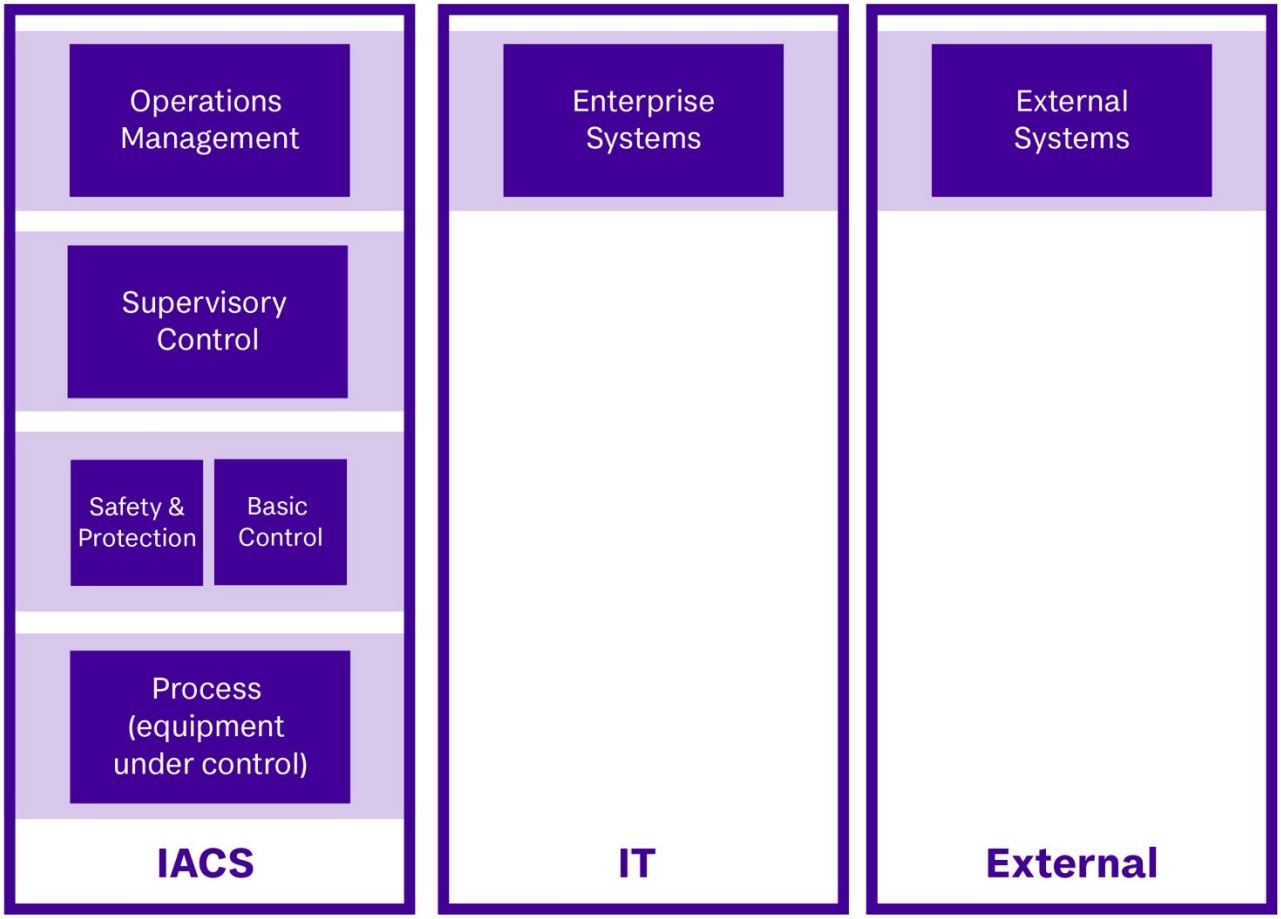

Figure 1 – Reference model[5]

A slightly different view of the reference model may be used for Supervisory Control and Data Acquisition (**SCADA**) applications as shown in figure 2:

[5] Adapted with modification from *IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*

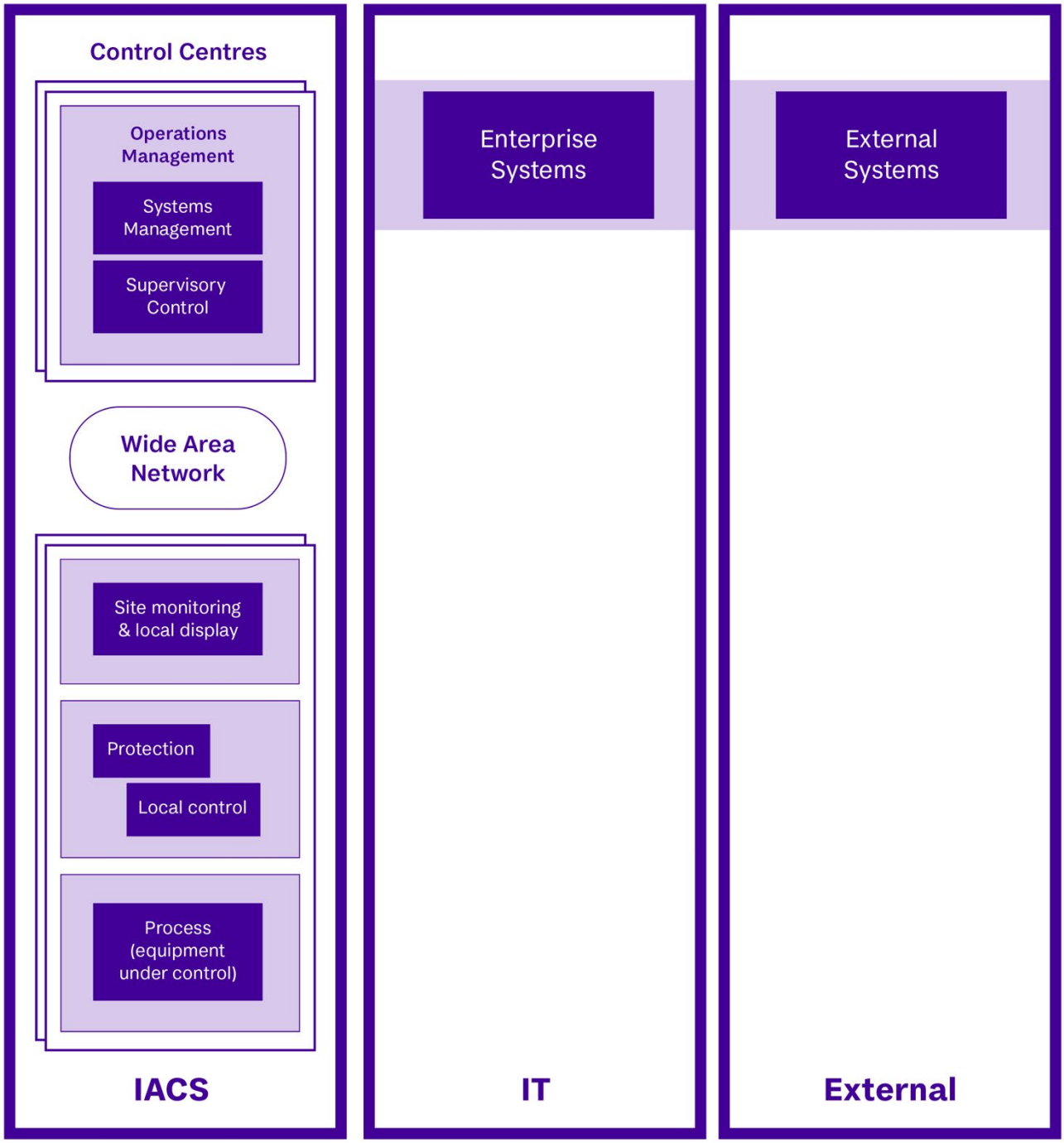

Figure 2 – SCADA Reference Model[6]

[6] Adapted with modification from *IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*

Standard 2 – Information Security Value

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 2 applies.

Additional IACS-specific Elements

V2.0 #	Element	Primary Source
E2.100	The organisation identifies, documents, and maintains the security attributes (confidentiality, integrity, and availability business impact levels) of its process automation assets in a register.	*IEC TS 62443-1-1:2009 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models* § 5.6.2 Assets § 6.5.4.3 Asset inventory

IACS-specific implementation guidance

Standard 2 is concerned with the security value of public sector information. Information can be categorised as a logical asset and is usually the focus of a security program in IT environments.

Information assets are generally technology agnostic and documented and maintained in an information asset register together with their security attributes (confidentiality, integrity, and availability (**CIA**) business impact levels (**BILs**)).

Process automation assets are a special form of logical assets specific to IACS environments. They contain the automation logic employed in executing industrial processes. These processes are highly dependent upon the repetitive or continuous execution of precisely defined events. Compromise of process assets can result in compromise to the integrity or availability of the process itself.

Process automation assets are usually an integral part of the physical technology assets they operate, therefore the security attributes of process automation assets should be documented and maintained in an appropriate register, such as existing physical asset inventories.

While the value of process automation assets is often assessed based on the impact on integrity and availability, the process itself may be proprietary and unauthorised disclosure (confidentiality) might lead to loss of intellectual property.

Standard 3 – Information Security Risk Management

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 3 applies.

IACS-specific implementation guidance

Operational IACS risk assessments are well established in IACS environments, with a focus on identifying, analysing, and evaluating risks to the reliability, availability, maintainability, and safety (**RAMS**) of IACS and the physical processes, machinery, and equipment they control.

The focus on the CIA of information in IACS information risk assessments is an emerging area. While similar or even identical terms (e.g., availability) are used in operational IACS and information risk assessments, different areas of the organisation identify, analyse, and evaluate risk in different ways.

The primary aim of an IACS information risk assessment is to support the operational objectives of IACS (**RAMS**) and the physical processes, machinery, and equipment they control, as shown in figure 3. An IACS information risk assessment may also identify risks directly related to enterprise IT or to public sector (including personal) information.

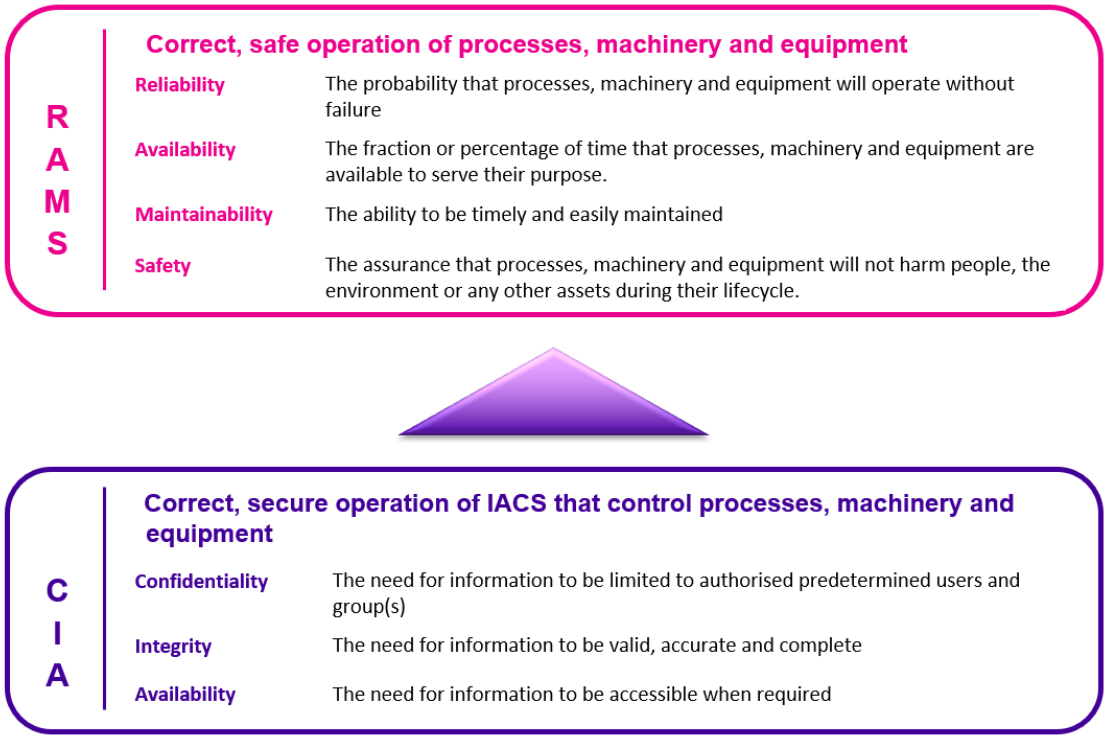

Figure 3 – How IACS information risk assessments support IACS and the processes, machinery, and equipment they control[7]

[7] Adapted with modification from the *Information Security Forum (**ISF**) Industrial Control Systems Report*

Standard 4 – Information Access

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 4 applies.

IACS-specific implementation guidance

The terms "information" and "IACS" can be used interchangeably depending on the environment.

Standard 5 – Information Security Obligations

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 5 applies.

IACS-specific implementation guidance

No additional guidance beyond that provided in *VPDSS Implementation Guidance V2.1.*

Standard 6 – Information Security Incident Management

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 6 applies.

IACS-specific implementation guidance

When developing and implementing information security incident management processes and plan(s), include both standard enterprise and IACS environments collectively.

Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 7 applies.

IACS-specific implementation guidance

No additional guidance beyond that provided in *VPDSS Implementation Guidance V2.1.*

Standard 8 – Third Party Arrangements

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 8 applies.

IACS-specific implementation guidance

Many organisations with IACS environments are reliant on specialised, or proprietary products and services from IACS suppliers who focus on functionality, often at the expense of information security.

IEC 62443-2-4 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers can be used by organisations to define and request specific security capabilities from the service provider.

More specifically, prior to such a request, IEC 62443-2-4 can be used by organisations to determine whether a specific service provider's security program includes the capabilities that the organisation needs.

It is recommended to consult the following as reference for requirement specifications:

- *IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*;
- *IEC 62443-4 Security for industrial automation and control systems* series:
    - *Part 4-1: Secure product development lifecycle requirements;* and
    - *Part 4-2: Technical security requirements for IACS components.*

Standard 9 – Information Security Reporting to OVIC

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 9 applies.

IACS-specific implementation guidance

When reporting to OVIC[8], include both standard enterprise IT and IACS environments collectively.

[8] Refer to OVIC's website for agency reporting obligations: https://ovic.vic.gov.au/agency-reporting-obligations-hub/

Standard 10 – Personnel Security

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 10 applies.

IACS-specific implementation guidance

No additional guidance beyond that provided in *VPDSS Implementation Guidance V2.1.*

Standard 11 – Information Communications Technology (ICT) Security

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 11 applies.

IACS-specific implementation guidance

Often an IACS consists of devices and systems from multiple vendors, all functioning together to provide the integrated automation functions for the industrial operation. Just as the functional capabilities of the individual devices contribute to the capability of the IACS, the security capabilities of the individual devices and implemented countermeasures need to function with each other to achieve a desired level of security for a zone.

A security zone is a logical grouping of physical, informational, and application assets sharing common security requirements.

IEC 62443 applies security concepts on a zone basis rather than on an individual device basis or system basis.

The concept of zoning in IACS may look similar to the concept of segregation applied in IT environments, but there are notable differences. Practitioners from each domain should develop an understanding of the concepts and differences of the other.

While the VPDSS Implementation Guidance V2.1 Elements remain unchanged for Standard 11, where the wording of the elements refers to "ICT", this should be read as including "IACS" as the context and environment requires.

Additional primary source references have been added below, designed for IACS environments to meet the security objective of each element.

V2.0 #	Element	Primary Source
E11.010	The organisation manages security documentation for its ICT systems (e.g., system security plans).	*IEC 62443-2-1:2010 Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program* § 4.3.4.3 Element: System development and maintenance

V2.0 #	Element	Primary Source
E11.020	The organisation manages all ICT assets (e.g., on-site, and off-site) throughout their lifecycle.	*IEC 62443-2-1* § 4.2.3 Element: Risk identification, classification and assessment
E11.030	The organisation conducts a security assessment for authorising systems to operate prior to transmitting, processing, or storing public sector information.	*IEC 62443-2-1* § 4.3.4.3.1 Define and test security functions and capabilities *IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels* § 7.5 SR 3.3 Security functionality verification
E11.040	The organisation undertakes risk-prioritised vulnerability management activities (e.g., patch management, penetration testing, continuous monitoring systems).	*IEC 62443-2-1* § A.2.3.3.2 Risk assessment and vulnerability assessment § A.2.3.3.8.7 Identifying vulnerabilities and prioritizing risks § A.3.4.2.5.2 Patching IACS Devices § A.3.4.3.7 Patch management *IEC TR 62443-2-3 Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment* All sections *IEC 62443-3-3* § 10.4 SR 6.2 Continuous monitoring

V2.0 #	Element	Primary Source
E11.050	The organisation documents and manages changes to ICT systems.	*IEC 62443-2-1* § 4.3.4.3.2 Develop and implement a change management system § 4.3.4.3.5 Integrate cyber security and process safety management (PSM) change management procedures *IEC 62443-2-1 Annex A (informative) Guidance for developing the elements of a CSMS* § A.3.3.5.3.12 Change management § A.3.4.3.6 Change management § A.4.2.2 Scheduled versus unscheduled activities
E11.060	The organisation manages communications security controls (e.g., cabling, telephony, radio, wireless networks).	*IEC 62443-2-1* § 4.3.3.4 Element: Network segmentation § A.3.3.3.2.8 Connections *IEC 62443-3-3* § 5.8 SR 1.6 Wireless access management § 6.4 SR 2.2 Wireless use control § 7.3 SR 3.1 Communication integrity § 11.3.3.2 SR 7.1 Denial of service protection

V2.0 #	Element	Primary Source
E11.070	The organisation verifies the vendors security claims before implementing security technologies.	*IEC 62443-2-4 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers* § 4.1.2 Use of IEC 62443-2-4 by IACS asset owners
E11.080	The organisation manages security measures (e.g., classification, labelling, usage, sanitisation, destruction, disposal) for media.	*ISM* § Guidelines for system management *IEC 62443-2-1* § A.3.3.3.2.12 Physical information § A.3.4.4.2 Considerations for information and document management *IEC 62443-3-3* § 6.5 SR 2.3 Use control for portable and mobile devices
E11.090	The organisation manages standard operating environments (**SOEs**) for all ICT assets, including end user access devices (e.g., workstations, mobile phones, laptops), network infrastructure, servers, and Internet of Things (**IoT**) commensurate with security risk.	*No additional primary source*
E11.100	The organisation manages security measures for email systems.	*IEC 62443-2-1* § A.3.3.4.2.2 Control zone *IEC 62443-3-3* § 9.5 SR 5.3 General purpose person-to-person communication restrictions

V2.0 #	Element	Primary Source
E11.110	The organisation logs system events and actively monitors these to detect potential security issues (e.g., intrusion detection/ prevention systems (**IDS/ IPS**)).	*IEC 62443-2-1* § 4.3.4.3 Element: System development and maintenance *IEC 62443-3-3* § 6.10 SR 2.8 Auditable events § 6.11 SR 2.9 Audit storage capacity § 6.12 SR 2.10 Response to audit processing failures § 10 FR 6 Timely response to events
E11.120	The organisation uses secure system administration practices.	*IEC 62443-2-1* § 4.3.4.3 Element: System development and maintenance *IEC 62443-3-3* § 4.4 Least privilege
E11.130	The organisation designs and configures the ICT network in a secure manner (e.g., segmentation, segregation, traffic management, default accounts).	*IEC TS 62443-1-1* § 5.12 Security level lifecycle *IEC 62443-3-3* § 5 FR 1 Identification and authentication control § 6 FR 2 Use control § 7 FR 3 System integrity § 8 FR 4 Data confidentiality § 9 FR 5 Restricted data flow

V2.0 #	Element	Primary Source
E11.140	The organisation manages a process for cryptographic keys (e.g., disk encryption, certificates).	*IEC 62443-3-3* § 8.5 SR 4.3 Use of cryptography
E11.150	The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation, and authentication commensurate with the risk to information.	*IEC 62443-3-3* § 8.5 SR 4.3 Use of cryptography
E11.160	The organisation manages malware prevention and detection software for ICT systems.	*IEC 62443-2-1* § 4.3.4.3.8 Establish and document antivirus/ malware management procedure *IEC 62443-3-3* § 7.4 SR 3.2 Malicious code protection
E11.170	The organisation segregates emerging systems from production systems (e.g., physical and/or logical) until their security controls are validated.	*IEC 62443-2-1* § A.3.4.3.5.6 System testing
E11.180	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).	*IEC 62443-2-1* § 4.3.2.5.6 Create backup procedures that support business continuity plan § 4.3.4.3.9 Establish backup and restoration procedure § A.3.4.3.8 Backup and recovery *IEC 62443-3-3* § 11.5 SR 7.3 Control system backup

V2.0 #	Element	Primary Source
E11.190	The organisation manages a secure development lifecycle covering all development activities (e.g., software, web-based applications, operational technology (Supervisory Control and Data Acquisition/ Industrial Control Systems (**SCADA**/**ICS**)).	*IEC 62443-2-1* § A.3.4.3 Element: System development and maintenance *IEC 62443-4-1 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements* All sections *IEC 62443-4-2 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components* All sections
E11.200	The organisation manages security measures for enterprise mobility (e.g., mobile device management, working from home).	*IEC 62443-3-3* § 6.5 SR 2.3 Use control for portable and mobile devices

Standard 12 – Physical Security

Standard

The standard from VPDSS applies.

Statement of Objective

The objective from VPDSS applies.

Elements

The implementation guidance from *VPDSS Implementation Guidance V2.1* Standard 12 applies.

IACS-specific implementation guidance

When selecting and implementing physical security measures, consider both standard enterprise and IACS environments collectively.

Appendix A - VPDSS Primary Sources

Primary Source	Link
Victorian Government - Office of the Victorian Information Commissioner	
Victorian Protective Data Security Standards (**VPDSS**) Implementation Guidance V2.1	https://ovic.vic.gov.au/data-protection/information-security-resources/
International Electrotechnical Commission (IEC) Please note: for eligible Victorian public sector organisations, access to some IEC documents is available free of charge and can be accessed from the Victorian Government Library Service (**VGLS**).	
IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and model	https://www.standards.org.au/standards-catalogue/international/iec-slash-tc--65/iec--ts--62443-1-1-colon-2009
IEC 62443-2-1:2010 Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program	https://www.standards.org.au/standards-catalogue/international/iec/iec--62443-2-1--ed-dot---1-dot-0
IEC TR 62443-2-3 Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment	https://www.standards.org.au/standards-catalogue/international/iec-slash-tc--65/iec--tr--62443-2-3-colon-2015
IEC 62443-2-4 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers	https://www.standards.org.au/standards-catalogue/international/iec-slash-tc--65/iec--62443-2-4-colon-2015
IEC 62443-3-2 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design	https://www.standards.org.au/standards-catalogue/international/iec-slash-tc--65/iec--62443-3-2-colon-2020
IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	https://www.standards.org.au/standards-catalogue/international/iec/iec--62443-3-3--ed1-dot-0
IEC 62443-4-1 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	https://www.standards.org.au/standards-catalogue/international/iec-slash-tc--65/iec--62443-4-1-colon-2018
IEC 62443-4-2 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	https://www.standards.org.au/standards-catalogue/international/iec-slash-tc--65/iec--62443-4-2-colon-2019

Primary Source	Link
Federal Government - *Australian Signals Directorate/ Australian Cyber Security Centre (**ACSC**)*	
Australian Government Information Security Manual (**ISM**)	https://www.cyber.gov.au/acsc/view-all-content/ism