ISO27001 Statement of Applicability

Reference	JATO-SEC-C.6.1.3d
Version	4.0
Publish Date	27/05/2026
Classification	**Public**
Author(s)	Head of Information Security
Owner	Chief Information Officer

PRINTED COPIES NOT CONTROLLED

JATO Dynamics Ltd, Building 1, The ARC, Sanderson Rd, Uxbridge, UB8 1DH, United Kingdom

Contents

1. Introduction 3
1.1 Document Scope 3
1.2 ISO27001 Requirements 3
1.3 Document Purpose 3
2. Organisational Controls 4
3. People Controls 12
4. Physical Controls 14
5. Technological Controls 17
6. ISO27001 Requirements Wording 24
7. Document Control 25
7.1 Revision History 25
7.2 Approval Details 25
7.3 Classification 25

1. Introduction

This **Public** document defines JATO's ISO27001 Statement of Applicability, which should be provided alongside JATO's official, accredited ISO27001 certificate. It has been created for any interested parties.

For additional details around sharing this document, please refer to the Classification section at the end.

1.1 Document Scope

This document covers all JATO companies and subsidiaries (hereafter referred to as the "Company") and applies to all JATO employees, staff, temporary workers, contractors and agents (hereafter referred to as "team members").

1.2 ISO27001 Requirements

This document is compliant with the following ISO/IEC 27001:2022 requirements:

a) Clause 6.1.3, Information security risk treatment.

1.3 Document Purpose

A Statement of Applicability should always be provided alongside any ISO27001 certificate. This document lists all ISO/IEC 27001:2022 Annex A controls and records if they apply to the scope of the Company's Information Security Management System (ISMS) or not. The Statement of Applicability is a fundamentally important document to the ISMS. It can also be used to record any additional controls that the Company has implemented (e.g. any required by customers).

The Statement of Applicability states a reason (or reasons) why each control applies to the Company and if it does not apply, provides a justification. Additionally, it provides the status of implementation for each control and a reason for including each control.

This document is compliant with a single point of ISO27001 Clause 6.1.3 (i.e. point d)). For additional and supporting information around this clause, please refer to the Company's Information Security Risk Assessment and Treatment Process (see separate document with reference JATO-SEC-C.6.1) and Information Security Risk Treatment Plan (see separate document with reference JATO-SEC-C.6.1.3).

The status of each control is selected from the following set of statuses:

a) Selected – Implemented;
b) Selected – Planned; or
c) Excluded.

The selection of reasons for including a control within the scope of the Company's ISMS are as follows:

d) Risk assessment (i.e. the control has been selected to treat an information security risk);
e) Operational (i.e. according to industry standards and best practices); and/or
f) Legislative (i.e. to comply with certain laws, data protection regulations, etc.)

2. Organisational Controls

A.5.1 Policies for information security

Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
4 June 2025
27 February 2025
13 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.2 Information security roles and responsibilities

Information security roles and responsibilities shall be defined and allocated according to the organizational needs.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
4 June 2025
27 February 2025
13 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.3 Segregation of duties

Conflicting duties and conflicting areas of responsibility shall be segregated.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
4 June 2025
27 February 2025
13 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.4 Management responsibilities

Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
4 June 2025
27 February 2025
13 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.5 Contact with authorities

The organization shall establish and maintain contact with relevant authorities.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
4 June 2025
27 February 2025
13 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.6 Contact with special interest groups

The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 27 February 2025, 13 June 2024, 20 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.7 Threat intelligence

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 27 February 2025, 13 June 2024, 20 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.8 Information security in project management

Information security shall be integrated into project management.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 27 February 2025, 13 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.9 Inventory of information and other associated assets

An inventory of information and other associated assets, including owners, shall be developed and maintained.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 25 February 2025, 14 June 2024, 20 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.10 Acceptable use of information and other associated assets

Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 25 February 2025, 14 June 2024, 20 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.11 Return of assets

Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
4 June 2025
25 February 2025
14 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.12 Classification of information

Information shall be classified according to the information security needs of the organization based on confidentiality, integrity and availability and relevant interested party requirements.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
4 June 2025
25 February 2025
14 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.13 Labelling of information

An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
4 June 2025
25 February 2025
14 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.14 Information transfer

Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
4 June 2025
25 February 2025
14 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.15 Access control

Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
4 June 2025
25 February 2025
14 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.16 Identity management

The full life cycle of identities shall be managed.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 25 February 2025, 14 June 2024, 20 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.17 Authentication information

Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 25 February 2025, 14 June 2024, 20 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.18 Access rights

Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 25 February 2025, 14 June 2024, 20 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.19 Information security in supplier relationships

Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 26 February 2025, 14 June 2024, 22 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.20 Addressing information security within supplier agreements

Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 26 February 2025, 14 June 2024, 22 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.21 Managing information security in the information and communication technology (ICT) supply chain

Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 26 February 2025, 14 June 2024, 22 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.22 Monitoring, review and change management of supplier services

The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 26 February 2025, 14 June 2024, 22 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.23 Information security for use of cloud services

Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 26 February 2025, 14 June 2024, 22 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.24 Information security incident management planning and preparation

The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 25 February 2025, 12 June 2024, 22 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.25 Assessment and decision on information security events

The organization shall assess information security events and decide if they are to be categorized as information security incidents.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 4 June 2025, 25 February 2025, 12 June 2024, 22 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.5.26 Response to information security incidents

Information security incidents shall be responded to in accordance with the documented procedures.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
4 June 2025
25 February 2025
12 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.27 Learning from information security incidents

Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
4 June 2025
25 February 2025
12 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.28 Collection of evidence

The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
4 June 2025
25 February 2025
12 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.29 Information security during disruption

The organization shall plan how to maintain information security at an appropriate level during disruption.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.30 ICT readiness for business continuity

ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.31 Legal, statutory, regulatory and contractual requirements

Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.32 Intellectual property rights

The organization shall implement appropriate procedures to protect intellectual property rights.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.33 Protection of records

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.34 Privacy and protection of personal identifiable information (PII)

The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.35 Independent review of information security

The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.36 Compliance with policies, rules and standards for information security

Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.5.37 Documented operating procedures

Operating procedures for information processing facilities shall be documented and made available to personnel who need them.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
6 June 2025
27 February 2025
12 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

3. People Controls

A.6.1 Screening

Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
6 June 2025
25 February 2025
7 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.6.2 Terms and conditions of employment

The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
25 February 2025
7 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.6.3 Information security awareness, education and training

Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
6 June 2025
25 February 2025
7 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.6.4 Disciplinary process

A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
25 February 2025
7 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.6.5 Responsibilities after termination or change of employment

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
25 February 2025
7 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.6.6 Confidentiality or non-disclosure agreements

Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
6 June 2025
25 February 2025
7 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.6.7 Remote working

Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
6 June 2025
25 February 2025
7 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.6.8 Information security event reporting

The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
6 June 2025
25 February 2025
7 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

4. Physical Controls

A.7.1 Physical security perimeters

Security perimeters shall be defined and used to protect areas that contain information and other associated assets.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 9 June 2025, 26 February 2025, 11 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.7.2 Physical entry

Secure areas shall be protected by appropriate entry controls and access points.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 9 June 2025, 26 February 2025, 11 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.7.3 Securing offices, rooms and facilities

Physical security for offices, rooms and facilities shall be designed and implemented.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 9 June 2025, 26 February 2025, 11 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.7.4 Physical security monitoring

Premises shall be continuously monitored for unauthorized physical access.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 9 June 2025, 26 February 2025, 11 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.7.5 Protecting against physical and environmental threats

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 9 June 2025, 26 February 2025, 11 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.7.6 Working in secure areas

Security measures for working in secure areas shall be designed and implemented.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.7.7 Clear desk and clear screen

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.7.8 Equipment siting and protection

Equipment shall be sited securely and protected.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.7.9 Security of assets off-premises

Off-site assets shall be protected.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.7.10 Storage media

Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.7.11 Supporting utilities

Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.7.12 Cabling security

Cables carrying power, data or supporting information services should be protected from interception, interference or damage.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.7.13 Equipment maintenance

Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.7.14 Secure disposal or re-use of equipment

Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
9 June 2025
26 February 2025
11 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

5. Technological Controls

A.8.1 User end point devices

Information stored on, processed by or accessible via user end point devices shall be protected.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.2 Privileged access rights

The allocation and use of privileged access rights shall be restricted and managed.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
25 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.3 Information access restriction

Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
25 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.4 Access to source code

Read and write access to source code, development tools and software libraries shall be appropriately managed.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
25 February 2025
17 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.5 Secure authentication

Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
25 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.6 Capacity management

The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.7 Protection against malware

Protection against malware shall be implemented and supported by appropriate user awareness.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.8 Management of technical vulnerabilities

Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.9 Configuration management

Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.10 Information deletion

Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.11 Data masking

Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.12 Data leakage prevention

Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.13 Information backup

Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
17 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.14 Redundancy of information processing facilities

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
10 June 2025
26 February 2025
17 June 2024
23 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.15 Logging

Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
27 February 2025
17 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.16 Monitoring activities

Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
27 February 2025
17 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.17 Clock synchronization

The clocks of information processing systems used by the organization shall be synchronized to approved time sources.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
19 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.18 Use of privileged utility programs

The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
19 June 2024
20 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.19 Installation of software on operational systems

Procedures and measures shall be implemented to securely manage software installation on operational systems.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
19 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.20 Networks security

Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
19 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.21 Security of network services

Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
19 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.22 Segregation of networks

Groups of information services, users and information systems shall be segregated in the organization's networks.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
19 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.23 Web filtering

Access to external websites shall be managed to reduce exposure to malicious content.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
19 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.24 Use of cryptography

Rules for effective use of cryptography, including cryptographic key management, shall be defined and implemented.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational
- Legislative

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
19 June 2024
22 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.25 Secure development life cycle

Rules for the secure development of software and systems shall be established and implemented.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
25 February 2025
18 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.26 Application security requirements

Information security requirements shall be identified, specified and approved when developing or acquiring applications.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 10 June 2025, 25 February 2025, 18 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.8.27 Secure system architecture and engineering principles

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 10 June 2025, 25 February 2025, 18 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.8.28 Secure coding

Secure coding principles shall be applied to software development.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 10 June 2025, 25 February 2025, 18 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.8.29 Security testing in development and acceptance

Security testing processes shall be defined and implemented in the development life cycle.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 10 June 2025, 25 February 2025, 18 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.8.30 Outsourced development

The organization shall direct, monitor and review the activities related to outsourced system development.

Status: Excluded
Reason(s) for exclusion: Development of the Company's products and services is not outsourced.
Date(s) of last independent review: n/a
Date(s) of next independent review: n/a

A.8.31 Separation of development, test and production environments

Development, testing and production environments shall be separated and secured.

Status: Selected – Implemented
Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review: 23-26 March 2026, 10 June 2025, 25 February 2025, 18 June 2024, 21 February 2024
Date(s) of next independent review: 27 May – 3 June 2026

A.8.32 Change management

Changes to information processing facilities and information systems shall be subject to change management processes.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
18 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.33 Test information

Test information shall be appropriately selected, protected and managed.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
25 February 2025
18 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

A.8.34 Protection of information systems during audit testing

Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.

Status: Selected – Implemented

Reason(s) for selection:
- Risk assessment
- Operational

Date(s) of last independent review:
23-26 March 2026
10 June 2025
26 February 2025
18 June 2024
21 February 2024

Date(s) of next independent review: 27 May – 3 June 2026

6. ISO27001 Requirements Wording

This section is included for reference purposes only and is not within the scope of this document (nor is it the Company's intellectual property). It includes the exact wording as published in the third edition of ISO/IEC 27001:2022.

6 Planning

6.1 Actions to address risks and opportunities

6.1.3 Information security risk treatment

The organisation shall define and apply an information security risk treatment process to:

d) produce a Statement of Applicability that contains;

- the necessary control (see 6.1.3 b) and c));
- justification for their inclusion;
- whether the necessary controls are implemented or not; and
- the justification for excluding any of the Annex A controls.

7. Document Control

7.1 Revision History

Version	Publish date	Changes	Author(s)	Owner
0.1 (DRAFT)	22 Jan 2024	New draft version created for review and approval based on latest document template. New unique reference number assigned (JATO-SEC-C.6.1.3d), classified as Public, author(s) and owner (for approval) assigned, document footer updated, cover page updated, contents table removed, section and sub-section numbering updated, formatting/layout updated for consistency, table/image numbers and captions added, Document Scope section updated, Document Purpose section updated, Roles and Responsibilities section removed, ISO27001 wording section updated, Document Control section updated, content added.	Information Security Manager	Head of Cyber Security
1.0	23 Jan 2024	Finalised and published version, approved by the Head of Cyber Security in email. Doc control sections updated, applicable comments removed and/or resolved, all changes accepted and tracked changes enabled.	Information Security Manager	Head of Cyber Security
1.1 (DRAFT)	26 Jan 2024	Draft version for review and approval. Status of controls updated ahead of internal audit. Doc control sections updated.	Information Security Manager	Head of Cyber Security
2.0	31 Jan 2024	Finalised and published version, approved by the Head of Cyber Security in email. Doc control sections updated, applicable comments removed and/or resolved, all changes accepted and tracked changes enabled.	Information Security Manager	Head of Cyber Security
2.1 (DRAFT)	15 Mar 2024	Draft version for review and approval. Updated status of 'Planned' controls (5.8, 5.13, 5.30, 5.31, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.8, 7.11, 7.12, 7.13, 8.10 and 8.24) to 'Implemented' following progress on new premises build and recent internal audit. Updated dates of last/next reviews. Updated document control sections.	Information Security Manager	Head of Cyber Security
3.0	25 Mar 2024	Finalised and published version, approved by the Head of Cyber Security in email. Doc control sections updated, applicable comments removed and/or resolved, all changes accepted and tracked changes enabled.	Information Security Manager	Head of Cyber Security
3.1 (DRAFT)	27 May 2026	Draft version for review and approval. Doc control sections updated, 'DRAFT' added to watermark, Company address in footer updated, changed document author, changed document owner (for review and approval process), changed "staff" to "team members" (following recent HR request), reviewed content for accuracy and suitability, updated details/dates of previous and future reviews, updated colour formatting for included/excluded controls, updated Contents table.	Head of Information Security	Chief Information Officer
4.0	27 May 2026	Finalised and published version, approved by the Chief Information Officer in email. 'DRAFT' removed from watermark, doc control sections updated, removed or resolved any applicable comments, accepted all changes, ensured tracked changes enabled.	Head of Information Security	Chief Information Officer

Table 1: Document revision history and details of changes.

7.2 Approval Details

This document has been formally approved by: Chief Information Officer
Approval method: Email
Date of approval: 27 May 2026

7.3 Classification

The Company has classified the information contained within this document as '**Public**'. This means that the information can be shared widely with no limitations on use. This information is intended for public use, freely available to all team memers and/or individuals or entities outside of the business and can be released outside of the business with no impact or associated risk.

No formal authorisation/approval to share this information is required by the owner of the information. Disclosure is not limited to individuals with confidentiality obligations within the Company and/or on a 'need-to-know' basis.

For further information please see the Company's Classification of Information Policy (separate document with reference JATO-SEC-A.5.12).