Information Security Policy

Reference	JATO-SEC-C.5.2
Version	7.0
Publish Date	08/05/2026
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 Status 3
1.3 ISO27001 Requirements 3
1.4 Document Purpose 3
1.5 Roles and Responsibilities 3
1.6 Compliance 4
2. Topic-Specific Policies 4
3. Scope of the Information Security Management System 4
4. Information Security Objectives 4
5. Policy 5
5.1 Exceptions 5
6. ISO27001 Requirements Wording 6
7. Document Control 7
7.1 Revision History 7
7.2 Approval Details 8
7.3 Classification 8

1. Introduction

This **Public** policy document outlines JATO's high-level rules and guidelines around information security. It has been provided for all JATO team members and any interested parties.

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

1.1 Document Scope

This policy 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").

This policy applies at all times to the processing (e.g. handling, labelling, management, sharing, administration, retention, etc.) of all information in scope of the Information Security Management System (ISMS), whether by electronic or manual methods.

1.2 Status

This policy does not form part of any team member's contract of employment and does not create contractual rights or obligations. It may be amended by the Company at any time.

1.3 ISO27001 Requirements

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

a) Clause 5.2, Policy.

1.4 Document Purpose

The Company's Information Security Policy should be considered as the 'master' (or high-level) policy for information security, which sets out top management's approach and commitment in this area. It is established, implemented and maintained by top management and as a foundation for the ISMS - covers key elements such as management and leadership buy-in and should be relevant to the purpose and context of the Company (see Context of the Organisation for more detail, i.e. separate document with reference JATO-SEC-C.4).

The master Information Security Policy should clearly communicate the intentions and strategic impact of information security and is supported by a number of separate, topic-specific (or low-level) policies, which provide more detail in specific areas (see later section for more details around these topic-specific policies).

The Information Security Policy should create a clear vision ensuring all interested parties understand the strategic direction of information security. Additionally, it should clarify the information security objectives of the Company. See later section for further details, and for more detailed information please see the Information Security Objectives (separate document with reference JATO-SEC-C.6.2).

1.5 Roles and Responsibilities

The Company sets out roles and responsibilities around the Information Security Policy as follows:

a) the Head of Information Security is responsible for maintaining and updating this policy;
b) the Chief Information Officer is responsible for approving and ensuring the suitability of this documented topic-specific policy;
c) readers are responsible for ensuring they are using the most up-to-date version of this document;
d) all team members and any relevant interested parties (e.g. third parties, suppliers, etc.) are responsible for complying with this policy;
e) top management is responsible for implementing and establishing this policy and ensuring the Company's compliance with it;
f) the Organisational Effectiveness Team are responsible for ensuring that this policy is communicated and made available to all team members; and
g) the Security Team are responsible for ensuring that this policy is made available for any relevant interested parties.

1.6 Compliance

Any non-compliance with or breach of this policy may lead to investigation and action in line with the Company's Disciplinary Process (for further information see separate document with reference JATO-SEC-A.6.4).

2. Topic-Specific Policies

As mentioned in an earlier section, a further subset of topic-specific policies relating to information security is available. In no particular order, these include topics such as (but not limited to):

a) clear desks and screens;
b) information security incidents;
c) passwords;
d) mobile devices;
e) malware;
f) access control;
g) acceptable use of information assets;
h) information backup;
i) cryptography;
j) secure development;
k) data retention;
l) secure disposal or reuse of equipment;
m) data protection;
n) business continuity;
o) vulnerability management;
p) information transfer;
q) third-party supplier relationships;
r) classification of information; and
s) remote working.

Topic-specific policies may be available as standalone documents, or included as sections in process documents. For more detail refer to Policies for Information Security (see separate document with reference JATO-SEC-A.5.1).

3. Scope of the Information Security Management System

The wording for the Company's scope of the Information Security Management System (ISMS), i.e. as per ISO27001 Clause 4.3 (Determining the scope of the information security management system), is as follows:

> *The certified scope of the Information Security Management System is applicable to JATO's systems and services being processed on their cloud platform, which supports the delivery of insight to customers through its global data analytics operations.*

For further information please refer to the Company's Context of the Organisation (see separate document with reference JATO-SEC-C.4).

4. Information Security Objectives

For more detailed information (e.g. responsibilities, frequency of measures, targets, due dates, etc.) then please refer to the Company's Information Security Objectives (see separate document with reference JATO-SEC-C.6.2).

A high-level summary of these objectives is included below:

a) high availability of the Company's Foundation products and services;
b) preserved confidentiality of the Company's and/or customer information;
c) preserved confidentiality of team members and/or customer personally identifiable information (PII);
d) preserved integrity of the Company's and/or customer information;
e) high and timely completion of mandatory team member security awareness training;
f) good phishing simulation results; and
g) regular and robust penetration testing of the Company's products.

5. Policy

It is the Company's policy to:

a) provide leadership and commitment from top management to preserve the confidentiality, integrity and availability of all information processed by the Company as appropriate for the context and purpose of the organisation;
b) develop secure, robust and reliable products and services for its customers;
c) comply with all applicable requirements related to information security including legal, regulatory, contractual and those defined in ISO27001;
d) maintain awareness throughout the Company and its supplier base of the importance of keeping information secure, whatever form that information may take (the Company achieves this in part via regular information security training and awareness programmes, and by remaining committed to meeting information security requirements);
e) stay at the forefront of developments in relation to information security by remaining vigilant to the ever-changing information security environment and by supporting a culture of Continual Improvement;
f) thoroughly address any nonconformity in relation to information security through appropriate corrective action by maintaining a robust non-conformance reporting system that is regularly reviewed;
g) provide necessary and proportionate resources in order to meet the Company's information security obligations through regular monitoring, measurement, analysis and evaluation of the ISMS;
h) facilitate Continual Improvement of the ISMS with such improvements made at appropriate times;
i) use best-practice cryptographic controls to encrypt data and devices wherever possible/feasible and to apply a pragmatic information classification scheme;
j) adopt a risk-based approach to information security by maintaining a current risk assessment process and risk treatment plan, which is reviewed not less than once a year; and
k) set and review information security objectives regularly at the Company's ISO27001 management review meetings (these objectives are communicated to all team members via the Company's training and awareness programmes and this policy).

5.1 Exceptions

An exception or exemption from this policy may only be granted by the Chief Information Officer or their designee. Examples of exceptions include (but are not limited to) the following circumstances:

a) implementation of a solution or system with equivalent protection to the requirements in this policy;
b) implementation of a solution or system with superior protection to the requirements in the policy;
c) impending retirement of a solution or system; or
d) inability to implement this policy due to limitation (e.g. technical constraint, business limitation, statutory requirement, etc.)

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.

5 Leadership

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security;

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization;

g) be available to interested parties, as appropriate.

7. Document Control

7.1 Revision History

Version	Publish date	Changes	Author	Owner
1.0 (DRAFT)	2 Jun 2017	INFS-PC-000. Draft version for review and approval. Change history not available.	Chief Security Officer	Chief Executive Officer
1.0	25 Jul 2017	INFS-DPA-001. Change history not available.	Chief Security Officer	Chief Executive Officer
1.2	19 Sep 2017	INFS-DPA-001. Change history not available.	Chief Security Officer	Chief Executive Officer
2.0	16 Aug 2019	INFOSEC-DPA-001. Change history not available.	Chief Security Officer	Chief Executive Officer
3.0	10 Aug 2021	INFOSEC-DPA-001. Change history not available.	Chief Security Officer	Chief Executive Officer
1.0	17 Feb 2022	INFOSEC-ISO-001. Change history not available.	Chief Security Officer	n/a
1.0	16 May 2023	INFOSEC-001. Change history not available.	Information Security Manager	Head of Cyber Security
1.1 (DRAFT)	8 Sep 2023	INFOSEC-001. Draft version for review and approval. Content reviewed by third-party consultants, ISO27001 controls section added.	Information Security Manager	Head of Cyber Security
4.0 (DRAFT)	19 Sep 2023	INFOSEC-014. Draft version for review and approval. Content reviewed by third-party consultants, ISO27001 controls section added, new unique reference number assigned.	Information Security Manager	Head of Cyber Security
4.1 (DRAFT)	9 Oct 2023	Draft version for review and approval created based on existing document template. Replaces all previous versions/issues of INFOSEC-001, INFOSEC-014, INFOSEC-DPA-001, INFOSEC-ISO-001, INFS-DPA-001 and INFS-PC-000. New unique reference number assigned (JATO-SEC-C.5.2), re-classified from Internal to Public (some earlier versions Confidential), author(s) and owner (for approval) re-assigned, document footer updated, cover page added, contents table added, section and sub-section numbering applied, formatting/layout updated for consistency, image and table numbers/captions added, content from latest versions reviewed by third-party consultants, Document Scope and Status sections added, Document Purpose section updated, Roles and Responsibilities section added, Topic-Specific Policies section added, ISMS Scope section added, Objectives section added, policy wording updated, Compliance section added, ISO27001 wording section added, Document Control section added, Definitions section removed, Publication section removed.	Information Security Manager, Head of Cyber Security	Chief Information Officer
5.0	11 Oct 2023	Finalised and published version, approved by the Chief Information Officer in email. Doc control sections updated, comments removed, accepted all changes and ensured tracked changes enabled.	Information Security Manager, Head of Cyber Security	Chief Information Officer
5.1 (DRAFT)	22 Oct 2024	Draft version for review and approval. Updated company address in footer, updated logo in template, moved Compliance section (for consistency), minor wording changes for improved clarity in Objectives section, updated Topic-Specific Policies section. Document control sections updated.	Information Security Manager, Head of Cyber Security	Chief Information Officer
6.0	15 Nov 2024	Finalised and published version, reviewed and approved by the Chief Information Officer in email. Doc control sections updated, comments removed, accepted all changes and ensured tracked changes enabled.	Information Security Manager, Head of Cyber Security	Chief Information Officer
6.1 (DRAFT)	4 May 2026	Draft version for review and approval. Added 'DRAFT' watermark, updated doc control sections, updated Company logo in header, replaced "staff" with "team members" (per HR request), updated document authors, updated Roles and Responsibilities section, checked document for accuracy and suitability.	Head of Information Security	Chief Information Officer
7.0	8 May 2026	Finalised and published version, reviewed and approved by the Chief Information Officer in email. Doc control sections updated, 'DRAFT' watermark removed, comments removed, accepted all changes and 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:	8 May 2026

7.3 Classification

The Company has classified the information contained within this document as '**Public**'. This means that the information can freely be made available outside of the business or is intended for public use. The information can be released outside of the business with no impact or associated risk.

No authorisation or approval is required from the owner of the information to share with any third party.

For further guidance and information around sensitivity and sharing of information, please refer to the Company's Classification of Information procedure (separate document with reference JATO-SEC-A.5.12).