Information Security Overview

An overview of information security at JATO, provided for existing or potential customers and any interested third parties. This document outlines JATO's approach to governance, risk and compliance around information security and JATO's platforms and solutions.

All rights reserved. © JATO Dynamics Ltd.

JATO Information Security Overview / Version 2.0 / July 2026

JATO-SEC-100

Public

Contents

Introduction 3

Document Purpose, Scope and Status 3

An Introduction to Us 3

Overview 3

Information Security Controls 4

Organisational 4

- Policy Management 4
- Roles and Responsibilities 4
- Threat Intelligence 5
- Asset Management 5
- Identity and Access Control 5
- Supply Chain Management 6
- Incident Management and Response 6
- Data Protection, Privacy, Legislation and Regulation 7

People 8

- Screening and Onboarding 8
- Security Training, Education and Awareness 8
- Business Code of Conduct 8

Physical Security 9

- Cloud Infrastructure 9
- Corporate Premises 9
- Secure Disposal of Data 9

Technological 10

- Endpoint Protection 10
- Management of Vulnerabilities 10
- Information Backup and Disaster Recovery 11
- Logging, Monitoring and Alerting 11
- Network Security 12
- Encryption 12
- System Acquisition, Development and Maintenance 13

Supporting Information 14

About us 15

Contacts 16

All rights reserved. © JATO Dynamics

Introduction

Document Purpose, Scope and Status

This document has been compiled for the benefit of JATO's customers and potential customers to help inform their supplier due diligence processes. It covers our key internal controls around governance, risk and compliance and principles that underpin the security of our data products and software solutions. This document should not be used for any other purpose, nor should reliance be placed on it by any other party.

Specific technical details of JATO's solutions, and principles and practices relating to our data processing activities are out of scope of this document but are available on request.

For the avoidance of doubt, the contents of this document are not intended to form part of any contractual relationship with a customer, and no express or implied warranties are intended to be given in it. The governance arrangements and controls identified herein are subject to change as JATO continues to evolve and improve its security posture consistent with best industry practice, its threat assessments and any independent accreditations.

An Introduction to Us

JATO Dynamics Ltd. is the world's leading provider of automotive business intelligence solutions. Since 1984, it has been our mission to help our customers maximise successfully achieving their business objectives by constantly leading in connected data, information and knowledge provision.

A selection of our products are offered as Software-as-a-Service (SaaS) solutions, delivered by our JATO-as-a-Service (JaaS) data platform. Other solutions provided by JATO are made available to customers through a variety of mechanisms and technologies.

Overview



JATO is ISO/IEC 27001:2022 certified (accredited), with a comprehensive and well documented Information Security Management System (ISMS) in place.

We follow industry best practices for security, including the use of strong encryption, multi-factor authentication, a secure software development lifecycle, extensive network security controls and comprehensive security monitoring and alerting. All of our employees are highly trained, both in their specific job role as well as in information security. JATO's systems and controls have been extensively assessed, audited and penetration tested by independent and accredited testers, certification authorities and experienced consultants using objective and globally-recognised assessment criteria.

JATO has suffered no data breaches or major security incidents to date.

All rights reserved. © JATO Dynamics

Information Security Controls

The following content provides details around key controls in place within JATO, arranged around the Annex A control sections of the ISO/IEC 27001:2022 international standard for information security. A copy of our accredited ISO 27001 certificate and Statement of Applicability (SoA) are available on request.

To protect the information that we are entrusted to manage, we utilise a defence-in-depth approach to implement layers of security controls throughout the business. The following sections and sub-sections describe a limited set of some of the most frequently asked about information security controls in place at JATO.



Organisational

Policy Management

To help keep all of our employees aware and up to date regarding information security requirements, we maintain a comprehensive suite of formalised, documented policies and procedures. As part of the ISMS, JATO maintains a high-level, or 'master', Information Security Policy, which covers a variety of topics such as (but not limited to) compliance with applicable legislation and regulation, considerations around privacy and data protection, encryption, Continual Improvement and the consequences for non-compliance.

The high-level policy is further supported with a subset of topic-specific policies covering a wide range of areas around information security such as access control, passwords, information backup, acceptable use, mobile devices, vulnerability management, remote working, etc.

All policies are reviewed and approved by top management at least annually and are stored on JATO's intranet where all employees have access to them. Any policies which require formal acknowledgment by employees are included in our mandatory training and awareness programmes. From the outset, compliance with corporate policies is embedded into the contracts and agreements of all of our employees and any third parties we work with.

Roles and Responsibilities

A full-time and experienced in-house team is responsible for all security matters within the Company on a day-to-day basis, with a dedicated Management Review Board (of which the Chief Information Officer and Head of Information Security are members) meeting on a regular basis to help set the overall security strategy and hold the business accountable. The board of directors is updated on security and compliance matters on a monthly basis.

Roles and responsibilities around information security are clearly defined across all levels of the business and are well documented in our policies and procedures. A clear segregation of duties is implemented at JATO across all applicable roles and departments with security being addressed on at least a weekly basis with all functional leads and heads of departments.

Ultimate accountability for information security lies with the Chief Information Officer and board of directors.

All rights reserved. © JATO Dynamics

Threat Intelligence

Through our managed Security Operations Centre (SOC), through the tooling we use and through a host of other external sources and contacts JATO maintains, we receive regular, reliable and up-to-date threat intelligence applicable to all areas of the business. Updates are timely, relevant, specific and keep JATO well-informed of the evolving threat landscape.

The comprehensive threat intelligence we receive is used to stay ahead of the game, to react where we need to and to ensure we are well prepared and can mitigate the risks associated with emerging threats, threat actors and any new or known vulnerabilities.

Asset Management

All of JATO's information assets are tightly controlled across the business throughout their complete lifecycle, with best practice tools and dedicated teams in place to manage these. A full IT asset register and inventory of information assets is maintained, regularly reviewed and updated, and where owners are clearly defined.

Per our policies, we classify information according to its sensitivity into one of several levels of classification (e.g. Confidential, Internal, Public, etc.) Each classification level has an associated set of training, handling and labelling requirements.

Identity and Access Control

JATO's suite of products and solutions allows for granular authorisation rules. Customers are provided with unique logins and are responsible for keeping their identities and passwords secure. Access to JATO API services are enabled through either API keys or OAuth (version 2.0) authorisation.

Within the business, all of our employees are issued with a unique identity. An extensive Access Control Policy is in place and enforced across the whole Company. Access to our corporate network (whether remotely through a VPN, or from within our premises) requires Multi-factor Authentication (MFA) and device validation. As per our policy, access to any of JATO's corporate systems is centralised via Single Sign-On (SSO).

JATO's well-defined policies around authentication information (such as passwords) follow industry best practices for required length, rotation frequency and complexity requirements.

Production Infrastructure Access

Access to JATO's production systems and infrastructure is strictly controlled and follows the principle of least privilege. Our employees are granted access using a role-based access control (RBAC) model.

Day-to-day access is minimised to only the individuals whose jobs require it. For emergency access (e.g. responses to alerts or troubleshooting) and access to administrative functions, JATO uses a Just-In-Time-Access (JITA) model through which authorised users can request access to privileged functions for a limited duration. Each JITA request is logged, and logs are continuously monitored and reviewed for anomalous requests. After the configured session limit, access to the account expires and is automatically revoked. Direct network connections to production infrastructure devices are prohibited, and engineers are required to authenticate first through a VPN connection before accessing QA or production environments.

All rights reserved. © JATO Dynamics

Privileged Access Rights

Additionally, all of JATO's system administrators have dedicated accounts for administrative work, separate from their normal user accounts. Administrator rights are managed through Privileged Identity Management (PIM), where elevated access must be requested, reviewed and approved (expiring after a set time). A full history of requests is maintained, and all other administrators are notified of any elevation of privileges. A four-eye/two-person rule has been adopted on all systems for any administrative activities involving users such as account creation, privilege changes, access revocation and support issues.

User Access Reviews

Manual reviews of access levels for user accounts take place regularly (i.e. monthly, quarterly, etc. depending on the sensitivity of data or criticality of system), across all systems with a full audit trail retained. Access levels are reviewed and approved by designated system owners. When an employee leaves JATO, their access to all physical, IT and cloud-based services is removed immediately as part of our robust joiners, movers and leavers processes.

Supply Chain Management

We use reputable, industry-standard third-party suppliers and service providers to support JATO's internal operations as well as the development of our products. These vendors demonstrate best industry practices and are independently accredited to international standards and compliance frameworks. Key suppliers' responses to security due diligence questionnaires are assessed to determine the level of information security risk they may pose and, where successful, to determine what controls and governance arrangements are appropriate for the relationship.

Our robust supplier relationship programme ensures that suppliers are never onboarded by a single employee: all supplier selection decisions require approval from the Chief Financial Officer following extensive legal reviews and risk assessments around information security. All supplier contracts are checked for robust data protection and confidentiality clauses, and where applicable – requirements around controls relating to information security. Additionally, any sub-contractor relationships are monitored and reviewed.

Incident Management and Response

JATO has well-defined and documented security incident management policies and procedures in place that detail the approach that will be taken to a security incident should one occur. This includes definitions of a security event or incident, key contacts, roles and responsibilities and escalation processes. Plans exist to deal with multiple different scenarios and detail the steps to be taken at each of the containment, eradication, and recovery stages of the incident. Communication plans are also detailed.

Between our experienced in-house SecOps team and managed third-party SOC service provider we are able to respond quickly to all information security events or incidents. Our key systems and a wide variety of automated processes feed into the incident management function including alerts, malicious activity, anomaly alerts or events, customer communications, etc. Industry-leading security tools (i.e. SIEM, SOAR, XDR, etc.) form the backbone of our ability to react quickly and effectively.

In the event of any incident affecting customer data, we would notify affected parties as soon as possible and no later than 24 hours after a breach or major incident is confirmed. Additionally, any lessons learned

All rights reserved. © JATO Dynamics

play a key part of our processes, with any information security incident (or 'near miss') being reviewed by top management as part of our compliance procedures and drive for Continual Improvement.

Data Protection, Privacy, Legislation and Regulation

JATO has a comprehensive data privacy and protection governance framework covering its processing of information to enable it to deliver its services. Aside from the information pertaining to our own employees, we do not process consumer personal data as part of the core services we offer. Any customer data which JATO is entrusted with is strictly limited and used solely for the purpose of providing our services, maintaining a business relationship and in the manner as outlined in contractual agreements with the relevant party, we do not assert any ownership over it.

The protection and privacy of our customers' information is one of our utmost considerations within our operations. As a cornerstone of our security programme, it is engrained in how we design and develop our solutions, the operational practices we put in place, the layers of protection we provide to reduce the risk of a single point of failure and any key legal, statutory or compliance certifications and attestations we need to meet. Crucially, and as described in our Privacy Notice (available on the website), we never sell or share personal data to any third party.

JATO Dynamics Ltd. is registered with the UK Information Commissioner's Office (ICO) and adheres (at a minimum) to the principles of the Data Protection Act 2018 and the UK GDPR. More information about this can be found on our corporate website. Any other entities authorised to use the name 'JATO' for the provision of services with whom customers may contract are appropriately registered with their respective local data privacy and protection regulators (where applicable) and comply with their respective local legal and regulatory frameworks.

Data Retention

We retain your information for as long you remain an active customer of JATO. Any information pertaining to former customers can be removed from our records upon request or after a defined period of time following termination of a contract or agreement.

JATO retains certain information such as metadata and related logs in order to better address any information security, compliance, legal or regulatory needs.

All rights reserved. © JATO Dynamics



People

The importance of information security, the 'human firewall' and a positive security culture are key ingredients to our ethos at JATO. Our employees are armed with clear, comprehensive and continually evolving policies, procedures and training. These are developed and maintained to inform those that work on our behalf about our expectations, and to provide them with the guidelines and our expected standards in acting in terms of security. This ensures our people remain up to date and at the forefront of the continuously changing threat landscape. All employees and anyone who works with us are required to sign a confidentiality agreement as part of their employment contract or agreement with JATO. This happens from the outset, and before any form of onboarding commences.

Screening and Onboarding

Prior to becoming part of our wider team, all new employees or contractors are subject to screening and background checks including identity, education, professional qualifications/certifications and (where applicable and dependant on any local employment laws) credit and criminal record checks. Any critical roles in system administration, security and/or top management are subject to enhanced screening checks performed by an independent third party.

Upon commencing employment, all of our employees must read and acknowledge JATO's Corporate Acceptable Use Policy (AUP). This helps define employees' security responsibilities in protecting Company assets/data (including, but not limited to, protecting mobile devices and securing corporate equipment). Employment contracts and agreements include explicit clauses stating our employees' obligations and responsibilities regarding information security.

Security Training, Education and Awareness

Our people are key to everything we do and form our 'human firewall' (they are our first line of defence). JATO invests heavily in the training and competence of those working on its behalf, including regular security awareness and education campaigns through computer-based courses and internal sessions. All of our employees are required to complete information security awareness training within four weeks of joining the team, with mandatory refresher training deployed on an annual basis (including content around data protection compliance). Additionally, smaller 'bite size' content is pushed out on a regular basis to targeted users within certain roles and departments.

Regular reminders are also sent out on various security topics, for example phishing and patching, through various internal communication channels as well as being discussed at regular Company meetings. In addition, a central training budget is allocated to help employees develop their job-related skills through classroom-based courses, by attending industry conferences and through online training subscriptions.

As well as the general security awareness training outlined above, we conduct phishing simulation campaigns on a monthly basis using industry-leading tools.

Business Code of Conduct

Our formally documented Business Code of Conduct outlines what is expected of everybody who works at, or on behalf of, JATO. All employees agree to the Code of Conduct, which they must formally acknowledge as part of their onboarding when they join our wider team (and whenever there's a change to it). It provides a

All rights reserved. © JATO Dynamics

set of principles that are adhered to and we encourage our people to respectfully challenge each other whenever this is not the case (building on our strong reporting culture).



Physical Security

Cloud Infrastructure

JATO does not host any product systems or data within the physical location of our corporate offices or premises. We outsource hosting of our product infrastructure to leading cloud infrastructure provider, Microsoft Azure.

Physical access to these data centres is strictly controlled, with a wide variety of physical and technological controls in place, tested regularly and validated by a broad range of globally-recognised certifications and accreditations available. Microsoft do not permit customers to have physical access to their Azure data centers. Azure maintains an audited security program, as well as physical, environmental and infrastructure security protections. JATO inherits the physical and infrastructure protections of Azure across all of its platforms.

For a full list of the comprehensive set of security certifications and accreditations maintained by Microsoft, please visit the Microsoft Compliance Offerings page, which is publicly available online.

Corporate Premises

Our corporate offices and premises are secured through a variety of robust measures and methods. Security services are employed at each of our international locations in order to provide a secure and safe environment for our people and our visitors. Secure entry points are leveraged, controlling access through unique RFID tokens issued to our employees.

Employees and visitors must wear an identity badge at all times, with a key card being used to gain access to our offices. Our headquarters are protected by 24x7 security personnel, CCTV and additional protective measures. A clear desk and screen policy is in operation and enforced across the Company.

All visitors to JATO's offices are escorted while on the premises and are required to sign in and out. A guest wireless network is available for visitors (where accepting terms before use is required), which is segregated from the main network.

Secure Disposal of Data

Within our cloud-hosted platforms, when a storage device has reached the end of its useful life, Microsoft Azure procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorised individuals. Azure use the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices.

For ICT equipment within our own sphere of control, we use the services of an accredited specialist data destruction company to securely dispose of all IT and iformation assets at the end of their lifecycle. Certificates of destruction are received for all equipment and media destroyed with a full audit trail kept. Any repurposed equipment undergoes rigorous internal procedures to securely wipe data.

All rights reserved. © JATO Dynamics



Technological

Endpoint Protection

We issue our employees with modern laptops and mobile devices which are managed centrally by dedicated teams of in-house experts. We ensure that software patches are applied in a timely fashion and adopt full use of a Mobile Device Management (MDM) system. This enables us to ensure that we can remotely wipe any device reported as lost or stolen in a timely fashion. Additionally, our systems provide us with the means to manage areas such as (but not limited to) configuration settings, installation of third-party applications and full-disk encryption (see later section for more detail around cryptography).

Our endpoints are further protected and secured by best practice Endpoint Detection and Response (EDR) solutions to help us continuously detect and monitor for any malicious or anomalous behaviour (including protection from viruses and malware).

DNS and email filtering is used to provide further protection against malicious software. Additionally, we maintain a comprehensive, documented Mobile Device Policy which ensures that our employees are kept up to date with the latest guidelines, techniques and best practices to protect our endpoints.

Management of Vulnerabilities

Key JATO systems are scanned automatically and continuously for technical vulnerabilities using industry-leading tools. We employ a combination of automated and manual scans across our infrastructure, networks, endpoints and the estate as a whole.

A robust technical vulnerability management programme is in place, managed by our teams of dedicated, full time employees and we maintain contact with specialist interest groups to stay up to speed with the ever-changing world of bad actors around us. High and critical vulnerabilities are assessed for impact and actioned as a matter of priority.

We operate a multi-layered approach to technical vulnerability scanning and management, using a variety of industry-recognised tools and techniques to ensure a comprehensive coverage of our technology environment. Vulnerability scanning is configured to search for exploitable vulnerabilities on a daily basis. Continuously running scans, along with constantly updated vulnerability detection signatures, helps JATO to stay ahead of the many security threats emerging from the threat landscape.

All of our hardware (including our endpoints and mobile devices) is kept within its support lifecycle with frequent firmware updates checked for and applied as a priority.

Penetration Testing

JATO also employs the services of industry-recognised, CREST-accredited third parties to perform regular (i.e. at least annual) penetration testing across the entire suite of our data products and software solutions. The objective of these programmes is to identify weaknesses which could pose information security risk and to rapidly address any issues found.

Additionally, our programme of penetration testing isn't just limited to the products and services we develop in house. We regularly enlist the services of independent, third-party experts to perform security testing and assessments on areas of our environment such as our physical premises, our networks and our websites.

All rights reserved. © JATO Dynamics

Code Scanning

In addition to the measures outlined above, our developed source code base is continuously scanned and assessed for vulnerabilities and flaws by a variety of tools and techniques. This helps us in managing the risks assosciated with the use of any external libraries, while ensuring that proprietary code is examined during the development process for common flaws such as SQL injection and cross-site scripting. By integrating these activities into our CI/CD pipelines we are able to ensure that both internal and external code components are scrutinised, leading to more secure and robust software applications.

Information Backup and Disaster Recovery

We ensure that all of our critical and customer-facing systems and the information associated with them are backed up regularly and we maintain a well-established frequency and schedule of performing these backups. Multiple days (and in certain instances weeks) of secure backups are maintained at JATO, and we do this in a manner which ensures that we can react quickly and easily to restore data.

We use robust tools and systems to ensure that all backups are monitored for succesful completion with an alerting system in place to generate and provide us with warnings should any exceptions arise. Any alerts which are generated to notify us of any failures or issues with our processes are escalated as a priority, investigated by the relevant teams and resolved as a matter of urgency.

Access to backup copies of information and databases is tightly managed in line with our documented Access Control Policy restrictions and associated procedures. All backups of production data are stored on highly available encrypted file storage facilities within Azure.

Operational data is backed up on at least a daily basis within the applicable local region. As an additional measure, backup copies are replicated to a separate Microsoft Azure region for recovery in the event of an outage in the primary region. Comprehensive monitoring and alerting processes are in place to detect any replication failures which are assessed and acted on accordingly. Business Continuity and Disaster Recovery plans for Azure have been independently validated as part of their ISO 27001 and SOC 2 Type 2 compliance certifications.

In addition to this (and in line with our own ISO 27001 compliance) – a business continuity and disaster recovery programme is in place to ensure that JATO's key service delivery functions can continue to operate (or be returned to operation) as quickly as possible in the event of a disruptive incident. It considers many scenarios including equipment failure or the loss of premises, with specific plans in place for all. It covers both our own corporate systems as well as those involved in the delivery of our solutions and services. Roles and responsibilities, communication plans and failover and alternative services are all covered, as well as definitions for recovery time and recovery point objectives. The plans are tested and reviewed at least twice annually, with outputs documented fully.

Our JaaS platform operates on the cloud, and as such - we benefit from geo-redundant storage of our backups. Further, this means that we do not utilise any form of physical media storage such as magnetic tapes or disks, removable media, paper, etc. Additionally, we have implemented processes to ensure that our backups are test restored on a regular basis (with a full audit trail maintained).

Logging, Monitoring and Alerting

Extensive logging and monitoring takes place on all of JATO's internal and third-party systems. Additional external alerting is configured using third-party monitoring services and other specialist interest groups.

All rights reserved. © JATO Dynamics

User and administrator activity is logged through the use of our Security Information and Event Management (SIEM) platform. Systems are monitored 24x7x365 using industry-standard tools, with alert notifications sent to both support teams and relevant security personnel.

Security events and user actions across our critical corporate systems and customer platforms are continuously added to and stored in logs. System logs are managed centrally and retained for defined periods of time in order to help us investigate and respond to potential information security incidents. The periods for which we retain logs will depend on the nature of the information being logged, but in any event this is typically a minimum of 90 days. Logs can be deleted earlier upon request or configured to retain for longer.

As a business, JATO has invested heavily throughout the years in automation. This also stems to our alerting and response functions in order to help us continuously address any potential issues. The JaaS platform (and our critical corporate systems) are configured to alert our system adminstrators and teams of experts when any anomaly occurs. These anomalies (such as alerts, attacks on applications, potentially malicious activity, errors, etc.) will subsequently generate automated responses and alerts which we ensure are received by the right people, best placed to act rapidly.

Network Security

All of JATO's networks are well documented and designed with redundant backups. We use modern firewalls with intrusion detection and prevention systems (IDS/IPS) at our premises, which have been deployed in a high availability architecture. We enforce system authorisation validation before allowing a device to connect to the corporate network. Any unauthorised devices are isolated from the network immediately. Any guest wireless networks are segregated from the corporate network for employees and systems, and the firewall is configured to block all inbound connections unless the session has been explicitly identified and is allowed.

All data transfers, whether with customers, partners or suppliers, are always performed using secure technologies such as SFTP or PGP encryption (as appropriate for the transfer being made).

The infrastructure of JATO's JaaS platform ensures that several layers of inspection and filtering of all connections throughout the platform are enforced. This includes our logical firewalls, Web Application Firewall (WAF) and security groups.

Network level access controls are implemented to prevent unauthorised network access to our internal product infrastructure. Firewalls are configured to deny network connections that are not explicitly authorised by default. Additionally, traffic monitoring is in place for detection of any anomalous activity.

Changes to our network security are actively monitored and controlled by mature change management processes. We review the rulesets of all firewalls regularly (i.e. on at least an annual basis) to help ensure that we have only configured necessary connections.

Encryption

All data is encrypted at rest using strong, industry-standard encryption techniques (i.e. AES 256). We encrypt all data in transit using TLS 1.2 or higher with strict Transport Layer Security across public networks. All of our servers and employee laptops have full hard drive encryption enforced per group policy with strong keys. All encryption keys are generated and securely managed by JATO; default or generic keys are strictly avoided as a matter of policy.

All rights reserved. © JATO Dynamics

JATO databases containing customer data are stored on encrypted volumes. Encryption is also enabled by default for all storage throughout the JaaS platform. Within our platform, all connections to storage locations or databases containing customer data are also encrypted using TLS 1.2 or above. Access to our infrastructure is limited to select JATO employees who can only reach it via MFA from a secure host.

System Acquisition, Development and Maintenance

Strong change management procedures are used by JATO. All changes must be documented (including an assessment of impacts and risks), reviewed by appropriate stakeholders and approved before being made in the development environment and put forward for testing.

No changes to the production environment can be made without first being tested by our extensive QA function, with only a limited number of senior employees authorised to implement any changes within the production environment.

Our solutions are maintained and developed in an active state with a Software Development Lifecycle (SDLC) in place. Any security vulnerabilities which are identified are patched following triage and risk assessment (where critical issues are typically patched as a matter of urgency).

Software Engineering

A Secure Software Development Lifecycle (SSDLC) has been implemented for the in-house development of all of our products. This includes performing threat modelling, using industry best practices such as OWASP, peer review of all source code and following secure principles for the selection and management of third-party libraries. All code is extensively tested in dedicated environments before being pushed to production. All software engineers and developers are experienced and receive ongoing training throughout their career with JATO. We do not outsource software development, all of our engineers work in-house and within the confines of our secure environments.

All rights reserved. © JATO Dynamics

Supporting Information

As stated earlier in this document, a copy of our accredited ISO 27001 certificate and Statement of Applicability (SoA) are available on request. We make these publicly available to anyone outside of the business who wishes to see them.

Our ISMS is based on the ISO/IEC 27001:2022 framework and includes a wide variety of further documented policies and procedures covering all aspects of our everyday operations at JATO. The following documentation can be shared after signing a non-disclosure agreement with us:

- Information Security Policy
- Policies for Information Security Process
- Artificial Intelligence (AI) Policy
- Information Security Roles and Responsibilities
- Contact with Authorities Process
- Contact with Special Interest Groups Process
- Acceptable Use Policy
- Classification of Information Policy
- Information Transfer Policy
- Access Control (Policy and Process)
- Password Policy
- Access Rights Process
- Information Security with Third-Party Suppliers (Policy and Process)
- Assessment and Decision on Information Security Events
- Information Security Incident Response Process
- Information Security Incident Response Playbooks (scenario-based)
- Learning From Information Security Incidents
- Collection of Evidence
- Business Continuity Plan (redacted)
- Data Retention Policy
- Data Protection Policy
- Employee and Staff Privacy Notice
- Personal Data Breach Notiifcation Process
- Screening Process
- Disciplinary Process
- Remote Working Policy
- Clear Desk and Clear Screen Policy
- Secure Disposal or Reuse of Equipment Policy
- Physical Security Controls (redacted)
- Mobile Device Policy
- Secure Software Development Lifecycle
- Management of Technical Vulnerabilities Process
- Information Backup (Policy and Process)
- Cryptography Policy
- Context of the Organisation
- Information Security Leadership and Commitment
- Organisational Roles, Responsibilities and Authorities
- Information Security Objectives
- Information Security Risk Assessment and Treatment Process
- Information Security Risk Treatment Plan (redacted)
- Information Security Management System Resources
- Information Security Competence Process
- Information Security Communications Process
- Information Security Documented Information
- Monitoring Measurement Analysis and Evaluation Process
- Internal Audit Process
- ISO 27001 Management Review Process
- Information Security Continual Improvement Process
- Information Security Nonconformity and Corrective Action Process

All rights reserved. © JATO Dynamics

About us

JATO Dynamics is the global leader in automotive data, analysis and intelligence. Our specialist solutions provide unmatched insights into the mobility industry and deliver clear perspectives in a complex market.

Covering the entire automotive lifecycle, we provide a detailed view of market dynamics, from product development and specifications to monthly payments and options uptake. With competitive intelligence on products, pricing and market positioning, we empower our customers to make strategic and commercially-driven decisions.

Our forward-focused approach includes substantial investment in technology, AI and our experts, allowing us to enhance competitive analysis. By combining timely data and industry knowledge, we enable our partners to grasp both early market trends and post-sale developments, answering the industry's most critical questions.

With comprehensive expertise across the automotive sector, we are a trusted partner for leading automakers, dealerships, digital marketplaces, leasing and fleet management companies and other mobility professional services. Whether your business needs precise market analysis or custom insights, our data-driven solutions can meet your requirements.

As we continue to innovate, JATO remains the partner you can trust to navigate and lead in the evolving automotive landscape.

Registered in England NO: 2262299.
Registered Office: JATO Dynamics Ltd
Building 1, ARC Uxbridge, Sanderson Road
Uxbridge, UB8 1DH

A-LIGN ISO 27001 CERTIFIED

Public

Contacts

+44 (0)20 8423 7100
securityinfo@jato.com

Visit us on social media:
Twitter: @JATO_Dynamics
Linkedin: linkedin.com/company/JATO-dynamics

JATO

Our Knowledge is Your Power

Registered in England NO: 2262299.
Registered Office: JATO Dynamics Ltd
Building 1, ARC Uxbridge, Sanderson Road
Uxbridge, UB8 1DH

A-LIGN ISO 27001 CERTIFIED