Policy & Transparency Statement

Artificial Intelligence & Machine Learning

Introduction

Our vision is that we build human centered Ai-powered solutions, which enable faster smarter decisions to create value for our communities.

We will deliver:

- Community Value – our deep understanding of community needs drives effective solutions
- Actionable Insights – data analytics and insights to drive smarter, faster decisions
- Ethical AI – a secure unified AI platform used for all solutions

This will be achieved through:

Incremental Adoption

We are integrating AI and machine learning into key areas of our product suite, balancing innovation with necessary safeguards to address risks.

Risk-based Approach

We recognise varying comfort levels with AI applications. We are implementing guardrails to reduce the likelihood of harm occurring in high-risk settings.

Continuous Evaluation

We actively research and invest in new AI tools to effectively and elegantly address customer business challenges, prioritising maturity, reliability and security.

Data & Governance

We constantly invest in evolving our Ai and data governance framework that guide our internal teams to design, build and deliver reliable, transparent and safe AI scenarios

Purpose

The purpose of this document is to provide guidelines and principles for the responsible, safe, ethical and secure development of AI/ML powered ERP solutions and to be transparent in our governance approach. Importantly, we continuously evaluate this AI/ML approach and our governance framework, prioritising maturity, reliability and security

Scope

This policy applies to all employees, contractors and third parties involved in the development, deployment and support of TechnologyOne's AI/ML powered solutions.

Guiding AI Principles

1. Create Value

TechnologyOne's AI/ML powered solutions will create value for our teams, customers, and the communities we serve. Our AI/ML-powered ERP solutions will:

- Make a tangible difference to our stakeholder's business practices by enhancing processes and supporting efficiency
- Focus on repetitive & low-value tasks, thus enabling stakeholders to perform higher-value work.
- Be resilient, sustainable, and able to withstand unexpected adverse events.
- Be tested for validity and perform reliably over the life of the system, and in line with our commitment to safety, security & quality

2. Create Collaboratively

We will take a considered, incremental approach to adopting AI/ML by consulting and collaborating with our stakeholders and customers, through proof of concept (POC) projects and early adopter (EA) programs.

Together we will ensure that AI-powered AI solutions:

- Are inclusive, fair, and accessible, ensuring the risk of harmful bias is mitigated at all stages including through development, optimisation, and operational stages
- Incorporate accountability and transparency, including indicating when AI powered functionality is in use.
- Provide traceability of data, processes, and decisions across all stages of tool use
- Provide the ability for customers to choose to use AI powered functionality, in line with their own organisational needs, values and context.
- Empower end users to self-serve, where possible, to manage the consumption and configuration, and addressing exceptions or errors.

3. Create Empathetically

Maintaining trust and meeting the expectations of our stakeholders is fundamental to successfully bringing our AI vision to life. Creating AI-powered solutions empathetically means we provide a range of technologies to enhance the way problems are solved, but in a respectful, considered way.

Our AI-powered solutions will:

- Avoid full automation in areas where human input is required or recommended to set rules, interpret results, or make critical decisions.
- Be created with integrity, ensuring tools are secure and safe, and comply with current and emerging AI, security, and privacy related laws.
- Enable our customers to comply with laws, standards and codes relevant to their business.
- Be risk-assessed prior to deployment and throughout the tool's lifecycle.
- Be designed to be robust, sustainable and perform as expected.

Transparency

The following sections provide transparency into our governance processes and use of AI:

Usage Patterns

Our software has incorporated AI/ML in the following ways:

- Workplace productivity – use of AI/ML tools to streamline ERP processes such as automated information extraction, summarisation, recommendations, natural language searches and a virtual assistant.
- Analytics for insights – use of AI/ML tools for data visualisation via natural language processing, forecasting and prediction.
- Image processing – processes images to automatically identify patterns and objects such as faces, buildings and objects.

Domains of AI Usage

TechnologyOne's application of AI/ML within our software includes:

- Service delivery - enhances efficiency or accuracy of business processes by providing tailored and responsive services. This may include in direct interaction with the public, such as chat-bots, enhanced customer self-service and multilingual capabilities, or support staff or systems which deliver services
- Corporate and enabling - supports corporate functions including HR and finance by automating processes, optimising resource allocation and improving operational efficiency.
- Compliance and fraud detection - identifies patterns or anomalies in data to detect fraudulent activities and ensure compliance with laws and regulations.

AI/ML Governance

TechnologyOne's AI/ML initiatives are overseen by our Chief Technology Officer (CTO) and our internal Risk, Compliance & Security (RCS) Council. The RCS Council is accountable for ensuring AI/ML initiatives are managed consistently, in line with our principles, policies and risk tolerances.

TechnologyOne has established an AI Management System framework aligned to ISO 42001:2023 and the Australian Voluntary AI Guardrails. This includes:

- Governance framework – a structured management framework for governing AI initiatives and related processes such as, AI development and data management.
- AI risk management – identification, assessment, evaluation, treatment and monitoring of risks associated with AI/ML.
- AI system impact assessments – identification and assessment of consequences of AI/ML systems to individuals, groups and/or societies.
- Continuous monitoring & improvement – monitoring AI/ML system performance to ensure it is operating as intended and continually improve performance over time
- Stakeholder engagement and transparency – continual communication with customers and other stakeholders to promote responsible use of AI.

Further details on our Governance Practices informed by ISO 42001 and the Australian Voluntary AI Guardrails can be found in Appendix A.

To ensure TechnologyOne's use of AI/ML tools aligns with the principles above and TechnologyOne's appetite for risk, internal teams must assess each AI-powered feature against a set of criteria, as summarised below:

Green Path: Proceed with caution

- Use case aligns with the guiding principles
- Use case maintains our security & compliance posture
- Use case aligns with strategic goals
- Use case is feasible

If the use-case meets the criteria above, it can proceed to the next stage of development, in line with our standard agile software development methodology.

Amber Path: Review, adjustment and/or consultation required

- Alignment with guiding principles is unclear or not all can be met
- Feasibility is uncertain
- Considered a 'high risk' model under AI/ML laws, directives, regulations, or standards

Where the proposed use case is on the 'Amber' path, teams are required to review the areas of misalignment and investigate alternatives to bring it back to the 'Green' path. Where alternatives have been exhausted, the CTO and/or the RCS Council, in consultation with subject matter experts, may make an exception and approve the use-case to proceed to the next stage. Exceptions and approvals are documented, and risks are recorded centrally.

Red Path: Do not proceed

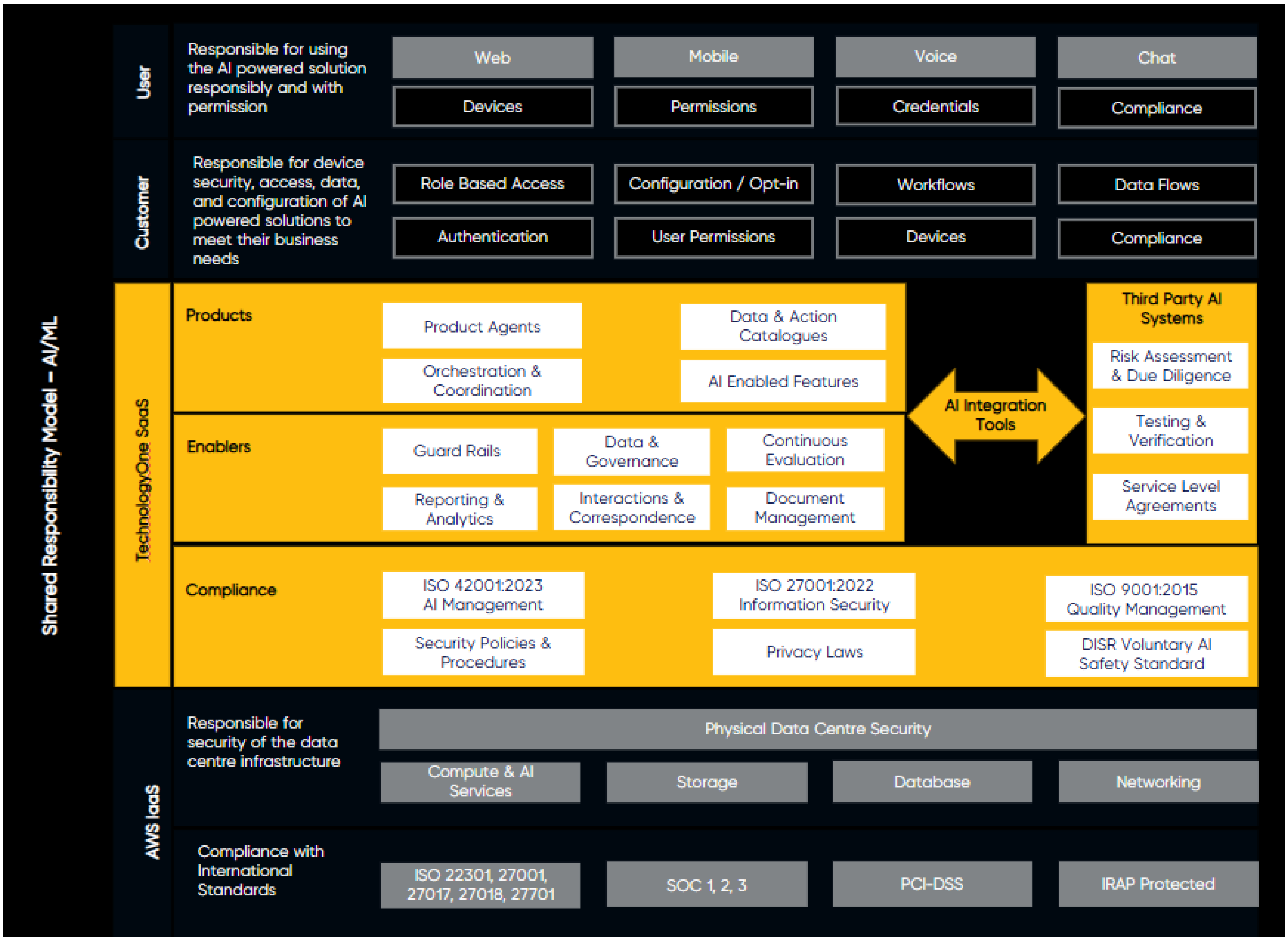
- Use case is not aligned with the guiding principles
- Use case is not feasible
- Considered a 'prohibited' model under AI/ML laws, directives, regulations, or standards

Where a proposed use case is on the 'Red' path, it cannot proceed unless there are material adjustments made in the use-case design or approach.

AI/ML Shared Responsibility Model

To ensure TechnologyOne's AI powered ERP solutions are trusted, secure, and safe to use, all parties will have a role to play in protecting the security and privacy of the data and systems used. The following diagram provides a summary of the various stakeholders and their responsibilities, in the context of TechnologyOne's AI powered solutions.

Shared Responsibility Model



Shared Responsibility Model – AI/ML

User

Responsible for using the AI powered solution responsibly and with permission

Web | Mobile | Voice | Chat

Devices | Permissions | Credentials | Compliance

Customer

Responsible for device security, access, data, and configuration of AI powered solutions to meet their business needs

Role Based Access | Configuration / Opt-in | Workflows | Data Flows

Authentication | User Permissions | Devices | Compliance

TechnologyOne SaaS

Products: Product Agents | Data & Action Catalogues | Orchestration & Coordination | AI Enabled Features

Enablers: Guard Rails | Data & Governance | Continuous Evaluation | Reporting & Analytics | Interactions & Correspondence | Document Management

AI Integration Tools

Third Party AI Systems: Risk Assessment & Due Diligence | Testing & Verification | Service Level Agreements

Compliance: ISO 42001:2023 AI Management | ISO 27001:2022 Information Security | ISO 9001:2015 Quality Management | Security Policies & Procedures | Privacy Laws | DISR Voluntary AI Safety Standard

AWS IaaS

Responsible for security of the data centre infrastructure

Physical Data Centre Security

Compute & AI Services | Storage | Database | Networking

Compliance with International Standards

ISO 22301, 27001, 27017, 27018, 27701 | SOC 1, 2, 3 | PCI-DSS | IRAP Protected

Further details of each set of responsibilities are provided below.:

User/Consumer

Users and/or consumers of the AI powered solutions are responsible for using the solutions responsibly and with permission, including:

- Protecting their credentials and using strong passwords
- Protecting the devices used to access the solutions
- Using the solutions in line with the permitted use and/or terms of service
- Abiding by the policies and procedures put in place by Customers

Customers

Customer responsibilities are a critical component of the control environment and are relied upon to ensure data and systems remain secure and safe.

Customer responsibilities are provided below. However, this should not be taken as a complete list of controls that are required to secure the customer's environment and/or data.

- The collection, use, storage, management, retention and deletion of all Customer production data.
- Reporting incidents and issues in a timely manner via the Customer Community, ensuring personal, sensitive or confidential data is obfuscated prior to requesting support.
- Configuring the roles, access, permissions, and authorisations of users, including authentication and password management.
- Configuring and testing prompts, determining when human input and oversight is required, and verifying the quality and accuracy of outputs
- Performing appropriate due diligence assessments and/or user acceptance testing (UAT) before using new or changed systems or functionality in production environments.
- Having policies and procedures in place to govern the use and access to data, applications and systems and monitoring compliance, and ensuring users are sufficiently trained and competent.
- Ensuring computing environments, including terminals, browsers and devices are physically secure, use up to date versions, and have cyber security controls applied.
- Ensuring security event logging rules and retention periods are defined, configured in the TechnologyOne application and reviewed periodically.
- Ensuring compliance with all legal, regulatory, contractual and compliance requirements relevant to the customer, including AI/ML related laws, standards and guardrails, anti-discrimination, consumer protection and privacy laws, and mandatory data breach notification requirements.
- Being transparent with their customers and/or end users about the use of AI/ML powered solutions.

It's also the customer's responsibility to ensure these controls are in place and they are working effectively.

TechnologyOne

TechnologyOne, as the Software as a Service (SaaS) provider, has the following responsibilities in the context of AI powered solutions:

- Creating value, working collaboratively and providing functions and features that add value and solve customer problems.
- Taking a risk-based approach, using guardrails to reduce the likelihood of harms occurring in high-risk settings. This includes performing governance activities, such as risk and security assessments, and third-party due diligence.
- Promptly acting upon reports of issues identified with the AI powered ERP solution, in line with the Customer Support Guide
- Ensuring compliance with laws, regulations, standards and contracts relevant to TechnologyOne, including AI/ML related laws, standards and guardrails, anti-discrimination, consumer protection and privacy laws, and mandatory data breach notification requirements.

- Completing system impact assessments
- Controlling and managing AI models and agents, and any shipped configuration associated with the use of AI/ML tools.
- Completing testing and verification procedures, in line with existing release management practices
- Continuous evaluation of model performance
- Setting and ensuring compliance with Service Level Agreements (SLA's) stipulated under supplier contracts
- Maintaining documentation and traceability pertaining to the use of data, models and agents.

For more information regarding TechnologyOne's general responsibilities as a SaaS provider, customers are encouraged to request our SOC 2 report by raising a Report Request in the Customer Community.

Amazon Web Services (AWS) Infrastructure as a Service (IaaS)

TechnologyOne leverages AWS's cloud computing platform infrastructure to deliver a SaaS Platform that is high performing, reliable and secure. AWS is responsible for:

- Providing TechnologyOne with compute, storage, database, and networking infrastructure services to suit TechnologyOne's needs.
- AWS is responsible for protecting the infrastructure that runs the services offered in the AWS Cloud, including the physical security controls to the platform infrastructure and AWS data centres.
- Maintaining a strong security posture and ensuring they continue to maintain compliance with international security standards.

Under no circumstances do AWS have access to TechnologyOne Customer data.

For more information regarding AWS's general responsibilities as an IaaS provider, customers are encouraged to request our SOC 2 report by raising a Report Request in the Customer Community.

Contact Us

If you require further information about this Policy, please contact the TechnologyOne RCS Council via:

- AIGovernance@technology1.com
- PO Box 96 Fortitude Valley, Queensland, 4006, Australia

Review and Updates

This Policy was last updated on 6 August 2025 It will be reviewed and updated annually or when significant changes occur.

Appendix A – Voluntary Guardrails

The following table describes how TechnologyOne aligns to the 10 Voluntary AI Guardrails published by the Australian Department of Industry, Science and Resources (DISR):

Guardrail	TechnologyOne approach
Guardrail 1: Establish, implement and publish an accountability process including governance, internal capability and a strategy for regulatory compliance.	TechnologyOne has established an artificial intelligence / machine learning strategy which is overseen by the Chief Technology Officer (CTO). The delivery of the strategy is supported by: • A dedicated team of AI/ML personnel experienced and skilled in the implementation of AI/ML tools and technologies • Existing internal procedures, such as the TechnologyOne agile product development process • AI governance framework which includes requirements to complete feasibility assessments and business cases, architectural and infrastructure design reviews, and security and compliance risk assessments • AI Governance Principles and assessment process to ensure alignment, as designs evolve. • Training and awareness activities, including regular communications, R&D All Hands meetings and other AI related learning events. Competency is assessed and managed through our existing Achievement planning framework, performance management procedures, and learning and development programs. • Internal assurance resources, who monitor compliance through internal and external audits.
Guardrail 2: Establish and implement a risk management process to identify and mitigate risks	TechnologyOne has an enterprise risk management process that includes risks related to the use and deployment of AI and ML enabled solutions. This is also supported with a Red, Amber and Green path framework for assessing individual AI/ML uses cases in the design phase during the AI lifecycle.

Guardrail	TechnologyOne approach
	Proposed AI/ML use cases undergo a system impact assessment in accordance with ISO 42001:2023 which assesses the impact of the solution to individuals, groups of individuals, or both and societies. AI systems and components delivered by an external third-party undergo a supplier risk assessment.
Guardrail 3: Protect AI systems and implement data governance measures to manage data quality and provenance.	TechnologyOne has an established Information security management system (ISMS) which encompasses security risks that result from the deployment of AI/ML solutions. Our SaaS platform is subject to frequent independent reviews to ensure we satisfy internationally recognised compliance standards and obligations, such as the Australian Cyber Security Centre (ACSC) Essential Eight Framework. Customers can request compliance certificates and reports by raising a report request in the Customer Community. including the Essential Eight Report. We have an active privacy compliance management program to ensure we meet the requirements of privacy laws in all operating regions. This includes a Privacy Policy that is reviewed periodically and a Security and Privacy Incident Response Plan (SPIRP) in place to meet our breach notification obligations in the regions that we operate in.
Guardrail 4: Test AI models and systems to evaluate model performance and monitor the system once deployed.	TechnologyOne has a software development framework aligned to the agile methodology which is applied to the AI/ML solutions we develop and release. This framework includes procedures for comprehensive testing of our products to ensure that solutions are reliable, secure and meet our customers' requirements. This includes but is not limited to: • Automated and manual testing; • Acceptance tests; • Testing requirements and acceptance criteria; • Penetration testing; and

Guardrail	TechnologyOne approach
	• Test plans containing scope, results of testing activities and any actions required. Customers can contact Support for concerns, challenges, bugs or other actions related to the use of AI/ML in the software either by raising a support case via the online Customer Community or by calling the Support team.
Guardrail 5: Enable human control or intervention in an AI system to achieve meaningful human over-sight across the life cycle.	TechnologyOne's AI/ML powered solutions are designed to ensure humans are in the loop in line with our guiding principles of 'Create Empathically'. Our intention is to avoid functionality with full automation in areas where human input is required or recommended to set rules, interpret results, or make critical decisions TechnologyOne has also established an AI management system ("AIMS") which has clearly defined roles, responsibilities, accountabilities and authorities. This includes roles responsibilities for: • AI/ML system development • Security and privacy incident response • Customer support • Testing and release of AI solutions As part of operating the AIMS, competencies of our personnel to deliver safe, secure and transparent AI systems and support our customers with their use is continually evaluated and managed.
Guardrail 6: Inform end-users regarding AI-enabled decisions, interactions with AI and AI-generated content.	Using our guiding AI/ML principles, we have incorporated transparency measures into the user interface (UI) of our AI solutions, so customers are aware when interacting with AI and provide the ability to opt out from its use.

Guardrail	TechnologyOne approach
Guardrail 7: Establish processes for people impacted by AI systems to challenge use or outcomes.	Customers can contact Support for concerns, challenges, bugs or other actions related to the use of AI/ML in the software either by raising a support case via the online Customer Community or by calling the Support team. When a new case is raised, it is triaged and then directed to the responsible team for investigation. Investigation activities consist of collecting any additional information and consulting within internal Research & Development teams. Concerns about the privacy of your information can be made to the Chief Privacy Officer as detailed in our Privacy Policy.
Guardrail 8: Be transparent with other organisations across the AI supply chain about data, models and systems to help them effectively address risks.	TechnologyOne is transparent with customers and other members of the supply chain regarding the use of AI/ML models and data management in the following ways: • By completing questionnaires, checklists and tender responses as part of the initial engagement process • During the contract signing and/or licensing process • By providing compliance certificates, reports and other artefacts (such as this AI Policy) upon request • By providing Release Notes when new functionality is deployed • Through knowledge articles and chat groups (available via the Customer Community) • Through the T1University • During the use of the AI/ML powered ERP solutions licensed to customers Our customers will be given the opportunity to assess the risks associated with TechnologyOne's AI/ML powered ERP solutions and opt-in during the contract negotiation and/or licensing phase, and where possible, while using the application software via the opt in / opt out features. Transparency

Guardrail	TechnologyOne approach
	is one of TechnologyOne's key AI Governance Principles. Being transparent with stakeholders is also a requirement under ISO 42001:2023.
Guardrail 9: Keep and maintain records to allow third parties to assess compliance with guardrails.	TechnologyOne maintains records of the AIMS as required under ISO 42001:2023 to allow our auditors to independently assess compliance with relevant standards. This includes but is not limited: • System documentation • Technical designs • Risk and impact assessments • Third party assessments • Testing results • Performance reporting
Guardrail 10: Engage your stakeholders and evaluate their needs and circumstances, with a focus on safety, diversity, inclusion and fairness.	Under our AIMS, we have identified and considered the needs and expectations of interested parties in the context of AI/ML. These needs and expectations have informed how we have designed our governance framework and how we perform risk and impact assessments. We perform system impact assessments which include the identification of individuals, groups and societies which may be impacted by the use of our AI/ML systems. Our AI Policy and associated guiding principles ensures our employees uphold and commit to the responsible development of AI/ML systems which do not undermine diversity, inclusion and fairness.

Glossary of Terms and Definitions

Term	Definition/Description	Examples
Artificial Intelligence System	Engineered system that generates output such as content, forecasts, recommendations or decisions for a given set of human-defined objectives	An engineered system designed to generate inventory forecasts and recommendations.
Machine Learning	A set of techniques that allows machines to improve their performance and generate models in an automated manner to identify patterns and regularities.	A machine learning system designed to detect fraudulent transactions based on patterns.
AI Agent	A system or program that autonomously performs specific tasks for a user	An AI agent designed to provide assistance and tailored recommendations when online shopping or browsing
Customer Production Data	The data or information entered into the production environment by the customer and the data used by the customer and/or their customer in their day-to-day operation of their business. This data typically contains confidential and person information collected by customers and is the most critical for a customer's business to operate. Thus, it is subject to the most stringent security controls and classified as either 'Secure' or 'Restricted Sensitive' under TechnologyOne's information classification policy.	Any information in a customer's environment, entered by the customer or their customer
Customers Meta Data	Metadata provides information about other data and is often used by monitoring tools or other applications to make working with specific data easier. In nearly all cases metadata lacks any identifiable characteristics of the underlying data and thus	Monitoring data, file size of systems, last modified dates, meta tags and labels

Term	Definition/Description	Examples
	poses minimal privacy concerns and low security risks. As such metadata is classified as 'Confidential' under TechnologyOne's information classification policy	
Customer Configuration Data	The configuration data for a customer is the information stored in our internal systems used to configure a customer's environment/apply the settings they have customised for their instances. As configuration data can be specialised to each customer there is a small but inherit risk that this specialised information could reveal information about a customer. As such configuration data is also classified as 'Secure' under TechnologyOne's information classification policy	Customers compliance domain information, customer instance size/type, CSP details for each unique customer, configuration tables unique to each customer
Model Training	Process to determine or to improve the parameters of a machine learning model, based on a machine learning algorithm by using training data	Improving the accuracy of an image detection system to identify different types of building structures
Testing	Verifying and validating that the designed and developed system operates in accordance with requirements and meets objectives.	Testing for ground truth accuracy over time – identifying model drift using known data sets and expected responses

Further Information and Contacts

For more information or to provide feedback about TechnologyOne's products, services, and our approach to privacy and security, refer to the following resources:

- TechnologyOne website via www.technology1.com
- Privacy Policy via www.technology1.com/privacy-policy
- SaaS+ Security via www.technology1.com/saas-plus/security
- Chief Privacy Officer via privacy@technology1.com
- AI Governance team via AIGovernance@technology1.com