DARKTRACE

Defend Beyond

■ darktrace.com

Darktrace - ISO 42001:2023 - Statement of Applicability v1.8

Reference	Control	Description	Implementation Status	Control Owner
A.2 - Policies Related to AI				
A.2.2	AI policy	The organization shall document a policy for the development or use of AI systems.	Full	Chief AI Officer
A.2.3	Alignment with other organizational policies	The organization shall determine where other policies can be affected by or apply to, the organization's objectives with respect to AI systems.	Full	Director Cybersecurity Compliance
A.2.4	Review of the AI policy	The AI policy shall be reviewed at planned intervals or additionally as needed to ensure its continuing suitability.	Full	AIMS Maintainer
A.3 - Internal Organisation				
A.3.2	AI roles and responsibilities	Roles and responsibilities for AI shall be defined and allocated according to the needs of the organization.	Full	Director Cybersecurity Compliance, AIMS Maintainer
A.3.3	Reporting of concerns	The organization shall define and put in place a process to report concerns about the organization's role with respect to an AI system throughout its life cycle.	Full	Chief AI Officer
A.4 - Resources for AI Systems				
A.4.2	Resource documentation	Data resources As part of resource identification, the organization shall document information about the data resources utilized for the AI system.	Full	Head of AI R&D
A.4.3	Data resources	Tooling resources As part of resource identification, the organization shall document information about the data resources utilized for the AI system.	Full	Head of AI R&D
A.4.4	Tooling resources	Tooling resources As part of resource identification, the organization shall document information about the tooling resources utilized for the AI system.	Full	Head of AI R&D
A.4.5	System and computing resources	As part of resource identification, the organization shall document information about the system and computing resources utilized for the AI system.	Full	Head of AI R&D

A.4.6	Human resources	As part of resource identification, the organization shall document information about the human resources and their competences utilized for the development, deployment, operation, change management, maintenance, transfer and decommissioning, as well as verification and integration of the AI system.	Full	Chief AI Officer
A.5 - Assessing Impacts of AI Systems				
A.5.2	AI system impact assessment process	The organization shall establish a process to assess the potential consequences for individuals or groups of individuals, or both, and societies that can result from the AI system throughout its life cycle.	Full	Director Cybersecurity Compliance, Chief AI Officer
A.5.3	Documentation of AI system impact assessments	The organization shall document the results of AI system impact assessments and retain results for a defined period.	Full	Director Cybersecurity Compliance, Chief AI Officer
A.5.4	Assessing AI system impact on individuals or groups of individuals	The organization shall assess and document the potential impacts of AI systems to individuals or groups of individuals throughout the system's life cycle.	Full	Director Cybersecurity Compliance, Chief AI Officer
A.5.5	Assessing societal impacts of AI systems	The organization shall assess and document the potential societal impacts of their AI systems throughout their life cycle.	Full	Director Cybersecurity Compliance, Chief AI Officer
A.6 - AI System Life Cycle				
A.6.1.2	Objectives for responsible development of AI system	The organization shall identify and document objectives to guide the responsible development AI systems, and those objectives into account and integrate measures to achieve them in the development life cycle.	Full	AIMS Maintainer
A.6.1.3	Processes for responsible AI system design and development	The organization shall define and document the specific processes for the responsible design and development of the AI system.	Full	AIMS Maintainer
A.6.2.2	AI system requirements and specification	The organization shall specify and document requirements for new AI systems or material enhancements to exisiting systems.	Full	Head of AI R&D
A.6.2.3	Documentation of AI system design and development	The organization shall document the AI system design and development based on organizational objectives, documented requirements and specification criteria	Full	Head of AI R&D
A.6.2.4	AI system verification and validation	The organization shall define and document verification and validation measures for the AI system and specify criteria for their use	Full	Head of AI R&D
A.6.2.5	AI system deployment	The organization shall document a deploymnet plan and ensure that apprpriate requirements are met prior to deployment	Full	Head of AI R&D
A.6.2.6	AI system operation and monitoring	The organization shall define and document the necessary elements for the ongoing operation of the AI system. At the minimum, this should include system and performance monitoring, repairs, updates and support.	Full	Head of AI R&D
A.6.2.7	AI system technical documentation	The organization shall determine what AI system technical documentation is needed for each relevant category of interested parties, such as users, partners, supervisory authorities, and provide the technical documentation to them in the appropriate form.	Full	Head of AI R&D
A.6.2.8	AI system recording of event logs	The organization shall determine at which phases of the AI system life cycle, record keeping of event logs should be enabled, but at the minimum when the AI system is in use.	Full	Head of AI R&D

A.7 - Data for AI Systems				
A.7.2	Data for development and enhancement of AI system	The organization shall define, document and implement data management processes related to the development of AI systems.	Full	Head of AI R&D
A.7.3	Acquisition of data	The organization shall determine and document details about the acquisition and selection of the data used in AI systems.	Full	Head of AI R&D
A.7.4	Quality of data for AI systems	The organization shall define and document requirements for data quality and ensure that data used to develop and operate the AI system meet those requirements.	Full	Head of AI R&D
A.7.5	Data provenance	The organization shall define and document a process for recording the provenance of data used in its AI systems over the life cycles of the data and the AI system.	Full	Head of AI R&D
A.7.6	Data preparation	The organization shall define and document its criteria for selecting data preparations and the data preparation methods to be used.	Full	Head of AI R&D
A.8 - Information for Interested Parties of AI Systems				
A.8.2	System documentation and information for users	The organization shall determine and provide the necessary information to users of the AI system.	Full	Head of AI R&D
A.8.3	External reporting	The organization shall provide capabilities for interested parties to report adverse impacts of the AI system.	Full	Director Cybersecurity Compliance
A.8.4	Communication of incidents	The organization shall determine and document a plan for communicating incidents to users of the AI system.	Full	Director Cybersecurity Compliance
A.8.5	Information for interested parties	The organization shall determine and document their obligations to reporting information about the AI system to interested parties.	Full	Director Cybersecurity Compliance
A.9 - Use of AI Systems				
A.9.2	Processes for responsible use of AI systems	The organization shall define and document the processes for the responsible use of AI systems.	Full	AIMS Maintainer
A.9.3	Objectives for responsible use of AI system	The organization shall identify and document objectives to guide the responsible use of AI systems.	Full	AIMS Maintainer
A.9.4	Intended use of the AI system	The organization shall ensure that the AI system is used according to the intended uses of the AI system and its accompanying documentation.	Full	AIMS Maintainer
A.10 - Third-Party and Customer Relationships				
A.10.2	Allocating responsibilities	The organization shall ensure that responsibilities within their AI system life cycle are allocated between the organization, its partners, suppliers, customers and third parties.	Full	Chief AI Officer
A.10.3	Suppliers	The organization shall establish a process to ensure that its usage of services, products or materials provided by suppliers aligns with the organization’s approach to the responsible development and use of AI systems.	Full	Information Security Manager
A.10.4	Customers	The organization shall ensure that its responsible approach to the development and use of AI systems considers their customer expectation and needs.	Full	Director Cybersecurity Compliance

<table>
<tr><th colspan="4">Issue Control</th></tr>
<tr><td><b>Issue</b></td><td>1.8</td><td><b>Date</b></td><td>19/11/2025</td></tr>
<tr><td><b>Classification</b></td><td>DLT0</td><td><b>Author</b></td><td>Director, Cybersecurity Compliance</td></tr>
<tr><td><b>Document Title</b></td><td colspan="3">Darktrace ISO 42001 Statement of Applicability - Customer Facing</td></tr>
<tr><td><b>Approved By</b></td><td colspan="3">Director, Cybersecurity Compliance</td></tr>
<tr><td><b>Released By</b></td><td colspan="3">Director, Cybersecurity Compliance</td></tr>
<tr><th colspan="4">Owner Details</th></tr>
<tr><td><b>Name</b></td><td colspan="3">Director, Cybersecurity Compliance</td></tr>
<tr><td><b>E-mail Address</b></td><td colspan="3">security@darktrace.com</td></tr>
</table>