Darktrace Corporate AI Policy

Table of Contents

1. Purpose

This Corporate AI Policy (Policy) establishes broad guidelines and best practices for the responsible and ethical use of Artificial Intelligence (AI) within Darktrace. It ensures that our employees and other personnel are using AI systems and platforms in a manner that aligns with Darktrace's values, adheres to legal and regulatory standards, and promotes the safety and well-being of interested parties.

Darktrace operates a full AI Management System (AIMS) aligned with the ISO 42001 standard that is supported and suitably resourced by Senior Management. The AIMS documentation greatly expands upon this concise Policy.

2. Scope

This policy applies to all employees, contractors, and partners of Darktrace (collectively referred to Darktrace personnel) who use or interact with AI systems. This includes but is not limited to relevant internal services, relevant external services including public LLMs, and Darktrace's own developed and deployed technology products.

3. Policy and Objectives

The overall objective is to ensure the responsible development and use of AI – within this framework more specific objectives are set.

3.1. Responsible AI Use

Darktrace personnel should use AI systems responsibly and ethically, avoiding any actions that could harm others, violate privacy, or facilitate malicious activities.

Darktrace personnel should consider and minimise the environmental impact of AI systems throughout the supply chain, where possible, promoting efficient use of computing resources and energy.

Darktrace personnel should ensure that the AI systems do not, under normal operational conditions, pose risks to human life or the environment. Elements of AI safety will be considered through our risk management process.

3.2. Compliance with Laws and Regulations

AI systems should be used in compliance with all applicable laws and regulations, including data protection, privacy, and intellectual property laws.

3.3. Transparency and Accountability

Darktrace personnel should be transparent about the use of AI in their work, ensuring that the business is aware of the technology's involvement in decision-making processes. Darktrace personnel should utilize Darktrace's AIMS to ensure transparency of proposed and active AI activities. Darktrace personnel are

responsible for the outcomes generated by AI systems and should be prepared to explain and justify those outcomes.

3.4. Data Privacy and Security

Darktrace personnel should adhere to the company's data privacy and security policies when using AI systems. They should ensure that any personal or sensitive data used by AI systems is appropriately anonymized and stored securely.

3.5. Bias and Fairness

Darktrace personnel should actively work to identify and mitigate biases in AI systems. They should ensure that these systems are fair, inclusive, and do not discriminate against any individuals or groups.

3.6. Human-AI Collaboration

Darktrace personnel should recognize the limitations of AI and always use their judgment when interpreting and acting on AI-generated recommendations. AI systems should be used as a tool to augment human decision-making, not replace it.

3.7. Training, Education and Expertise

Darktrace personnel who use AI systems should receive appropriate training on how to use them responsibly and effectively. They should also stay informed about advances in AI technology and potential ethical concerns.

Darktrace ensures that AI systems are assessed, developed and deployed by dedicated specialists with appropriate skill sets.

Competence is ensured through hiring requirements, vetting process and interviews. Darktrace personnel involved in the research and development of AI systems are encouraged to stay up to date with emerging methods and technologies, as required.

3.8. Third-Party Services

When utilizing third-party AI services or platforms, Darktrace personnel should ensure that the providers adhere to the same ethical standards and legal requirements as outlined in this policy. There is a separate policy (GAI1 Use of Generative AI policy) which contains important restrictions on the use of generative AI services. Please consult that policy for additional information.

3.9. Data Quality, Maintainability and Robustness

Darktrace personnel should ensure that the AI systems are trained and tested using relevant, representative and high-quality data. Data quality is ensured through our responsible AI development and data management processes.

Darktrace personnel should design AI systems that are maintainable and updatable, ensuring ongoing performance, compliance and adaptability to new requirements.

Darktrace personnel should ensure AI systems are resilient to errors, adversarial inputs and misuse, maintaining reliable performance under varying operational conditions. Robustness is verified through our testing and performance evaluation process.

4. Implementation and Monitoring

4.1. AI Governance

A multidisciplinary AI risk management team comprised of a diverse team of experts, including data scientists, legal and compliance professionals will ensure that AI initiatives are developed and deployed responsibly, in compliance with relevant laws and regulations, and with ethical considerations in mind. There are defined roles and responsibilities for designated people critical to the oversight of Darktrace's AI initiatives.

4.2. Designated AI Officer

A designated Chief AI Officer will be responsible for overseeing the implementation of this policy, ensuring guidance and support is available to Darktrace personnel, and driving compliance with relevant laws and regulations.

4.3. AI Impact Assessments and Risks

AI system impact assessments are undertaken as part of the development of Darktrace's products. A Risk Register maintains the known AI risks to the business, their controls and any active treatment plans.

4.4. AI Supplier Assessments

AI supplier assessments are undertaken as part of the vendor risk management process where suppliers, services or systems offer AI functionality.

4.5. AI Program Reviews

Periodic reviews of the AIMS will be conducted within the company to ensure adherence to this policy, identify any emerging risks, and recommend updates to the AIMS as necessary.

4.6. AI Concern Reporting and Exceptions

Any observed or suspected issue, behaviour or outcome involving an AI system that raises potential ethical, legal, regulatory, privacy or environmental risks should be reported to **aiconcernreporting@darktrace.com** in accordance with AIMS01 AI Concern Reporting Procedure.

If anonymity is desired, it can also follow organisation's Whistleblowing policy.

Any suspected violation of this policy, including any requests for exceptions, should be reported through the same reporting channels.

Technical issues involving AI systems such as problematic detections, integration or functionality errors, model drift or degradation in performance, change requests and feature requests should be reported via product engineering channels.

5. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment or contractual engagement, in accordance with Darktrace's disciplinary policies and procedures.

6. Policy Review

This Policy will be reviewed annually or as needed, based on the evolution of AI technology and the regulatory landscape. The wider AIMS has ongoing development, reviews and audits.

7. Commitments

Darktrace commits to following this Policy, meeting all applicable requirements related to the development and use of AI, and continually operating and improving the AI Management System.

Jill Popelka
Chief Executive Officer
Darktrace Limited
11th August 2025

Jack Stockdale
Chief Technology Officer
Darktrace Limited
11th August 2025

Tim Bazalgette
Chief AI Officer
Darktrace Limited
11th August 2025

Document Control

Issue Control			
Document Reference		**Project Number**	
Issue	2.0	**Date**	11/08/2025
Classification	DTL0	**Author**	AIMS Maintainer
Document Title	Darktrace Corporate AI Policy		
Approved by	AIMS Maintainer		
Policy Owner	AIMS Maintainer		

Revision History				
Issue	**Date**	**Author**	**Distribution Channel**	**Comments**
2.0	11/08/2025	AIMS Maintainer	The POD	Update to AI Objectives
1.2	17/06/2025	AIMS Maintainer	The POD	Update to AI concern reporting process
1.1	27/11/2024	AIMS Maintainer	The POD	Refer to specific objectives
1.0	12/11/2024	AIMS Maintainer	The POD	Initial version