DARKTRACE

Information Security Policy

Table of Contents

Document Control

This is a controlled document produced by Darktrace. The control and release of this document is the responsibility of the Darktrace document owner. This includes any amendment that may be required.

Issue Control			
Document Reference	ISP	Project Number	
Issue	5.1	Date	10/03/2025
Classification	DTL0	Author	Security Compliance Manager
Document Title	Information Security Policy		
Approved by	Global CISO		
Released by	Security Compliance Manager		

Owner Details	
Name	Security Compliance Manager
Office/Region	
Contact Number	
E-mail Address	security@darktrace.com

Revision History		
Issue	Date	Comments
5.1	10/03/2025	Amendments to Organisational Security sections
5.0	09/10/2024	Updated for 2024
4.0	21/08/2023	Review and amendments (new ISO 27001 standard)
3.2	24/07/2023	Updated for 2023
3.1	20/02/2023	Amendments to Section 19
3.0	01/07/2022	Updated for 2022

Purpose

The purpose of this policy is to outline the approach to information security adopted by Darktrace. This policy is intended to provide an overview of the information security management system (ISMS) and the security procedures in place to ensure the confidentiality, integrity and availability of information controlled or processed by Darktrace.

Scope

This policy is applicable to all employees, including consultants, temporary staff, contractors, secondees and all other persons who may access or make use of the organisation's information resources and systems. This policy applies to all business activities, processes and functions within the organisation.

ISMS

The ISMS ensures security of all information controlled or processed by Darktrace, and all its affiliates ("Darktrace"). This is achieved through policies, procedures and controls.

The ISMS is driven by the organisation's security strategy, which is defined and agreed at the executive management level. The Security Team maintains an ISMS Manual, further outlining the scope, requirements, resources, interested parties and management of the ISMS.

Roles and responsibilities for the ISMS have been defined, approved and communicated to the Executive Team, Security Team, and leadership representatives from across the organisation. Responsibilities are detailed in information security and privacy policies, as well as our organisational chart.

Objectives & Our Approach to Information Security

Darktrace's ultimate security goal is to:

Establish a premier cybersecurity program that not only protects our digital assets but also ensures the utmost security and privacy of our customers' data. Guided by Darktrace's ISO27001, ISO 27018, and Cyber Essentials certification, and working within the risk boundaries set in our public risk statement, we are committed to creating a resilient and compliant information security management system (ISMS) that supports our mission of providing cutting-edge cybersecurity solutions to our global customer base.

Darktrace intends to achieve this goal with security objectives that are outlined in the OBJ1 Security Objectives document.

CEO Statement

Jill Popelka

Chief Executive Officer

"As CEO of Darktrace I give complete approval and commitment to this policy, ensuring Darktrace meets all applicable requirements related to information security, complies with applicable PII and privacy protection legislation, adheres to contractual terms within customer contracts and ultimately places the protection of customer data at the heart of our information processes.

We are deeply committed to the continual improvement of the information security management system, as demonstrated by our ISO 27001 and ISO 27018 certifications.

Our security program ensures data confidentiality, integrity and availability is effectively maintained with robust administrative, technical and physical security controls across the entire organization."

Jill Popelka

Jill Popelka
CEO
Darktrace Limited
9th October 2024

CISO Statement

Mike Beck

Global CISO

“As the Chief Information Security Officer at Darktrace, I am deeply committed to ensuring that our security philosophy is fully aligned to industry best practice. Central to our approach is the belief that proactive, adaptive defences powered by advanced machine learning and AI technologies are key to protecting our customers against sophisticated cyber threats. By fully leveraging the Darktrace product suite, we aim to stay ahead of potential attackers, continuously learning and evolving our defences in response to new and emerging threats. This innovative approach allows us to offer unparalleled protection, ensuring that our customers' systems are secure against both known and unknown threats.

At the same time, we recognize the importance of balancing engineering innovation with best practice risk management. To this end, we implement a rigorous vetting process for all third-party vendors and partners, ensuring that they meet our high standards for security. This includes comprehensive risk assessments and regular audits to maintain a secure supply chain. Our commitment to data privacy and security is unwavering, and we employ the strongest encryption methods and follow strict access controls to safeguard our customers' information. By integrating these practices with our cutting-edge AI and machine learning technologies, we provide a robust security framework that not only reacts to threats but anticipates them.

With customers located all over the world, Darktrace holds governance and transparency in the highest regard, recognizing these principles as foundational to earning and maintaining the trust of our customers, investors, and the broader community. Our commitment to governance is evidenced through our adherence to rigorous regulatory standards and ethical business practices.”

Management Commitment

Darktrace executive management recognises that information security must be upheld by the management team to support and achieve our security objectives. Darktrace Management has approved the Information Security Policy and agreed the information security and privacy objectives, including methods of performance measurement.

Executive management has also committed to providing the resources required to operate the Information Security Management System (ISMS), and work towards the information security and privacy objectives agreed. Resources include, but are not limited to, financial, time, expertise, knowledge or authority/support.

Security Team

Darktrace prides itself on the expertise, capability and experience demonstrated by our Security Team. Our Security Team is championed by our Global CISO, based out of London, and includes members based across the UK, US, Netherlands and Australia, providing 24/7 coverage. Alongside an enterprise-wide Darktrace deployment, our Security Team helps to protect Darktrace from ever-evolving security threats, protecting our employee data, customer data and intellectual property of Darktrace.

The Security Team compromises of:

- **Security Operations Centre (SOC)** - Responsible for the identification, analysis and containment of security events and incidents, enabled by our utilisation of our industry leading Darktrace tooling, and supporting platforms.

- **Security Architecture & Engineering** – Responsible for the Secure by Design governance, vulnerability management platform and internal penetration tests against our internal environment.

- **Security Compliance** – Responsible for the management and oversight of our Information Security Management System (ISMS), security certifications, data governance and continual improvement procedures.

- **Information Security** – Responsible for the Third-Party Information Security Assurance Program (TPISA), information security risk management, change control and information security best practices in project management.

- **Red Team** – Responsible for Red Team exercises, identification of threats, adversary simulation and technical assessments against our internal environment and Darktrace tooling.

At Darktrace, we make certain that strong security principles and best practices are at the core of all our teams. We achieve this by working closely with every department, ensuring we drive strong security practices.

Every Darktrace employee upholds our commitment to information security, with ample resources, knowledge and training available to everyone, and is supported by our Security Team.

Continual Improvement

Darktrace makes a commitment to the continual improvement of our Information Security Management System (ISMS).

Ensuring that we enable continual improvement, Darktrace has elected to certify to the ISO 27001 standard, setting a strong foundation for information security management. Adopting this approach allows for independent assessment and attestation that our information security controls are operating effectively and continually maturing.

Darktrace has also elected to carry out additional independent assessments in the form of internal audits with an external assessor throughout the year, covering our whole ISMS and products.

The Security Team closely monitors the performance of the ISMS, benchmarking against industry 'gold' standards and internal objectives set by management. Defined metrics support the monitoring of security performance and are reviewed by Security Management and Executive Teams. Metrics are used to identify and target opportunities for improvement across each of our control domains.

Darktrace executive management makes a commitment to providing the resources required to support a continually improving ISMS.

Organisational Security

Access Control

Darktrace ensures that all access to systems, assets, data and customer environments is monitored, authorised and controlled based upon the following principles:

- Need-to-know: you are only granted access to the information you need to perform your tasks.

- Need-to-use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role (least privilege).

A formally documented Access Control Policy is maintained by the IT Group and Security Team. Darktrace shall log or document access requests and authorisations. Access to systems is regularly reviewed, to ensure that users are still authorised to access each system. The Security Team requests that system administrators, or provisioners, review the accesses for which they are responsible. Responses to electronic access reviews will be returned to the Security Team and evidence noted.

Privileged Access reviews are conducted, and results are centrally recorded.

Access to the organisation's networks shall be limited to prevent unauthorised and unintended purposes. Devices will not be connected to the organisation's network without authorisation from designated approvers in either the Security Team or IT Group. Access requests must be submitted to the IT Team, with Security Team approval where necessary. A list of Security, IT and Development approvers is maintained, and reviewed on an annual basis.

Darktrace utilises a Zero Trust solution to provide secure, remote access to all enterprise applications, including utilising two-factor-authentication as standard across the business. Unauthorised devices are technically restricted from joining internal networks via a combination of device-based conditional access policies and Darktrace /NETWORK™, /ENDPOINT™ and /IDENTITY™. Wi-Fi connection details are not shared without authorisation from the Security Team.

Access removal requirements and procedures are outlined in the Access Control Policy.

User activity is logged and routinely monitored for the purposes of error detection and security. The Security Team maintains necessary and proportionate levels of security monitoring coverage across the enterprise, including SaaS systems, on-premise infrastructure, and cloud environments.

Privileged Access

The use of privileged accounts (admin/root) will be limited, operating on 'need to know' and 'need-to-use' principles. All privileged access should be reviewed against the job function before the details or assets (including access cards) are issued to the user. This is at the discretion of the IT Group, Security Team or CTO as advised by the HR department.

Uniquely identifiable usernames will be used to enable all activity under an account to be traced back to a single individual. No default administrative passwords will be left unchanged. Hardware tokens are required for administrative roles. The Security Team performs quarterly privileged access reviews.

Visitor Access

Guests, visitors and third parties must follow the Visitor Access Policy. This includes only connecting to 'Guest' wireless networks. Unknown contractors working on, or near, network or IT equipment must be escorted at all times. Known contractors may work unescorted, except in sensitive areas, and must have their physical access limited appropriately to their work requirements.

All visitors are required to wear 'visitor' lanyards, provided by the Reception Team upon arrival.

Network Segregation

Darktrace uses physical and logical segregation of networks. To protect source code, the core software development network is physically separate to all other internal networks. The 'Guest' wireless network is physically separate to the corporate wireless network.

Login Security

Users must authentication using a unique user ID, password and a multi-factor authentication (MFA) token. MFA is required for remote access to all critical systems. Identity governance is managed alongside the organisation's zero trust secure networking solution, which regularly confirms the identity of the user to ensure authorised access to core systems. SaaS systems utilised by Darktrace will only be used in production where the requirements of the SaaS Data Security Policy are met.

Passwords

Darktrace enforces strict password complexity requirements for all employee devices and user accounts. Passwords are required to access systems transmitting, processing or storing customer data. Passwords are set in line with guidance from National Cyber Security Centre (NCSC) and the National Institute of Standards and Technology (NIST). In general, all accounts must have a unique password, with a minimum length of 12 characters. Further information is outlined in the Password Policy.

Employees are provided with a secure password manager specifically so that not all passwords have to be memorised. Passwords must not be written down under any circumstance. Where passwords are required to be shared for non-human accounts, security forward practices are followed, as outlined by the Password Policy.

Asset Management

A full asset inventory database is maintained by the IT Group / Security Team for all devices, including those both with and without network access. Device ownership is assigned to a specific user in the database with a continual review and update cycle. A separate asset database is kept for customer appliances.

The asset database updates automatically as part of the staff exit process. An Exit Certification Form certifies the return of assets and re-confirms the relevant provisions. Offboarding procedures are outlined in more detail in the Asset Management Policy.

All data stored on physical information assets classified as hardware must be fully wiped prior to disposal. Assets will be disposed of by the certified partner in line with guidelines dictated in the Data Destruction Policy.

Business Continuity Planning

A plan has been developed to provide continuity in the event of a long-term total effective loss of Darktrace product services, network infrastructure, communications services, and working locations. The Business Continuity Plan (BCP) is updated and re-approved annually by BCP Manager, Executive Team, Security Team and IT Group.

Services supporting key business functions and staff teams have been identified. Each service has at least two members of staff assigned with the knowledge, skills and access required, as well as a documented recovery procedure developed in advance.

Each service has a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) set by the BCP Manager and system/function owner in support of customer instance resiliency and redundancy.

Disaster Recovery

Darktrace operates several critical internal systems which directly support customer services and deployments. These are managed and tested in line with the Business Continuity Plan.

For cloud-hosted customer services and deployments, Darktrace leverages the resiliency and redundancy measures offered within selected CSP availability zones to provide an uninterrupted service. Darktrace Cloud Masters operate out of one Availability Zone (AZ) within a particular cloud region. AZs consist of one or more discrete data centres, each with redundant power, networking and connectivity, housed in separate facilities. In the event of an outage, the AZ model means that the loss of availability is only confined to that particular data centre. If an AZ is offline for a prolonged period of time, the Darktrace backup and restore process takes into account that backups span multiple AZs, allowing the Cloud Master to be restored into another AZ within the same region. Data will not restore outside of the agreed cloud region.

In the event of loss of availability for Darktrace products and supporting services operated from the Cambridge HQ, services will resume (fail over) to a Darktrace owned disaster recovery site. The site is located within the United Kingdom and is geographically diverse to the Cambridge HQ.

Business Continuity and Disaster Recovery Testing

Elements of the Business Continuity Plan are tested routinely throughout the year to maximise testing value, identify remediation actions and ensuring resilience in business operations with regards to customer services and deployments. Testing can include dry runs, tabletop exercises or full, live tests. Any remediations are identified, consolidated, logged and addressed in the subsequent tests.

Change Management

Darktrace operates a formal change control program. All changes are risk assessed and recorded within the ticketing system. Capacity management, where limitations exist, is tracked. Only late-stage testing occurs on a staging server in operational environments. Operational networks are logically segregated. Changes in production systems, infrastructure or code is subject to the change control program, as outlined in the Secure Engineering Principles document.

Cloud Security

Public CSPs provide critical infrastructure to support some of Darktrace's core business operations. Cloud security is governed collaboratively between Security, IT and Development teams.

Use of cloud (i.e., SaaS, PaaS, IaaS) platforms must comply with the requirements outlined in the SaaS Data Security Policy, Use of Public Cloud Policy, Third-Party Collaboration Policy and the requirements outlined in this document. Darktrace will ensure that use of cloud complies with all applicable regulatory and compliance requirements, as well as adhering to industry best practices, ensuring the risks typically associated with cloud are managed.

Darktrace cloud environments that process customer data (most notably personally identifiable information) are built, managed and governed by the requirements outlined in ISO/IEC 27018:2019, for which Darktrace is certified to.

In addition, leveraging CSP-native security controls, Darktrace requires that the following security requirements are adhered, and applied, to all Darktrace cloud systems or environments:

- Authentication: Single Sign-On (SSO, with two-factor authentication (2FA) must be enabled for access to all cloud environments. 2FA must be used for both privileged and nonprivileged accounts.

- Product: Darktrace Cloud Security products must be deployed in all cloud environments, where required.

- Encryption: Data is encrypted both at rest and in transit.

- Network Security: Web application firewalls (WAFs) must be deployed on all applicable public cloud environments at the network perimeters.

At the time of decommissioning existing cloud computing services, the business owners shall address matters of data retention, decommissioning of cloud infrastructure and outstanding contractual considerations, and these should be captured by the Security or Systems Operations teams and any residual risks treated.

Cloud-Hosted Deployments

Cloud-hosted deployments of Darktrace products utilise hosted datacentres provided by Microsoft Azure, Amazon AWS or Google Cloud Platform (GCP). Microsoft Azure, Amazon AWS and GCP are sub-processers of Darktrace. Customers can choose specific regions for Darktrace cloud services to be deployed in. This is covered in depth within Darktrace's Master Hosted Terms.

Web Security

All web/HTML interfaces offered by Darktrace internally and externally must meet the minimum standards set out in the Web Security policy. Darktrace websites are designed to avoid the OWASP Top 10 vulnerabilities. Input validation and escaping must be handled by a recognised feature of the chosen platform or a trusted library. No inline scripting is used in new sites, in support of the CSP header restrictions.

All web interfaces that serve data of any sensitivity or require authentication are served over HTTPS using modern, secure cipher suites. At the time of writing, the server's first preferred cipher suite is summarised as: TLS v1.3 protocol, AES with 128-bit key in GCM mode encryption, a pseudo-random function of TLS PRF (with SHA-256), authentication using ECDSA-256 with SHA-256 on P-256 curve, and a key exchange using ECDHE using P-256 curve. In particular, the following cipher suites are disabled: SSL v2/v3, TLS v1.0, RC4, DES, MD5. All external-facing web applications use an external trusted certificate authority. Publicly accessible websites are protected by anti-DDoS hosts.

Vulnerability Management

Darktrace Internal Security and Development Teams remain abreast of security notifications for any underlying libraries and platforms and will push out patches as part of the regular product or system updates.

Within development environments, Darktrace leverages Python and NPM security tools to identify weaknesses, misconfigurations and vulnerabilities.

The Darktrace Security Team leverages a combination of open and closed-source vulnerability scanners, as well as its own /NETWORK™, /ENDPOINT™, /IDENTITY™ and /CLOUD™ products. These tools enable the security team to identify and prioritize high-risk vulnerabilities and misconfigurations affecting its IT infrastructure.

Auto-updates are enabled wherever possible and auto-update capabilities are frequently reviewed for accuracy and efficacy. Devices and services that are unable to receive auto-updates are patched as soon as possible after vulnerability disclosure or during the next scheduled monthly update window.

Vulnerability scanning of internal and external infrastructure is performed monthly, and endpoints are scanned on a continuous basis. Vulnerability findings with a CVSS severity of CRITICAL or HIGH (>= 7) will be fixed within 7 days. Findings of MEDIUM (>= 4) will be addressed by an automatic update within 30 days. LOW (< 4) findings will be addressed as part of the monthly patch cycle. Exploitable vulnerabilities affecting internet facing infrastructure are patched within 72 hours of disclosure.

Penetration Tests

On an annual basis Darktrace will perform a full penetration test against core Darktrace products. New major versions of Darktrace products will undergo penetration testing, leveraging internal resources and/or an external security assessment firm. Qualified internal penetration testers will implement the Open Web Application Security (OWASP) Testing Methodology for web application security assessments. As a globally recognised and adopted framework, the OWASP methodology provided an exhaustive and structured approach to identifying and mitigating security risks in web applications. Darktrace will remediate findings and make a redacted report available for customers to review.

For internally developed functions, systems are tested by a qualified penetration tester before a new application or system is put into the production phase, before each major version release, or at regular scheduled intervals. Internal penetration testing will contain, but not be limited to:

- A full enumeration phase, whereby all open ports and services are scanned for vulnerabilities and misconfigurations.
- A combination of both thorough manual and automated testing using a wide variety of tooling, dependent on the output of the enumeration phase.
- A detailed and full report of all vulnerability findings found within the system.

Vulnerability Disclosure Policy

Darktrace maintains an external Vulnerability Disclosure program, covering Darktrace Appliances and Darktrace Sensors. The Security and Development Teams will actively triage submissions. Researchers who submit a vulnerability report to us will be given full credit in the release notes once the submission has been accepted and validated by our product security team. More information can be found on our website: darktrace.com/legal/vulnerability-disclosure-policy.

Testing Remediation Standard

Results from testing activities will be presented in order of severity, using a recognised industry standard scoring system such as CVSS.

Vulnerabilities and penetration testing findings with a severity of CRITICAL or HIGH (>=

7 CVSS) will be fixed as soon as practicable, but no later than 7 days from identification.

For Darktrace products, the complete test will be repeated until no such findings remain before the version is released to customers. MEDIUM (>= 4) findings will be addressed be addressed within 30 days, preferably with an automatic update deployed to customers if concerning Darktrace products.

LOW (< 4) findings will be addressed before the next major system or product release.

Configuration Management

A configuration management program has been established, ensuring Darktrace's hardware, software, services and networks function as intended while adhering to any security settings. System owners are responsible for configuration management and adherence to all applicable policies.

Secure Development Lifecycle

All Darktrace products and internally developed systems are developed with secure engineering principles and security by design methodologies in place. Darktrace commits to the inclusion of security requirements at all stages of the software development lifecycle (SDLC).

Darktrace operates a development environment which is physically separate from the rest of the internal network. This network is hardened with a next generation firewall, secure access requires MFA over a Zero Trust Network Access solution, and privileges are tightly controlled. Darktrace maintains an internal Secure Engineering Principles Policy to outline best practice.

All open-source usage, whether the open source is used internally, as part of the Darktrace's products, or as part of a web service, needs to be reviewed through the OSS approval process.

Darktrace operates a regular, collaborative DevSecOps forum and a monitored communication channel comprising of senior individuals from Development, IT Group and Security. Engineering workload requests in the design phase, technical changes and process considerations around software development are assessed alongside an information security risk assessment if applicable.

Darktrace has established a compliance framework in the development environment, which overlays all development groups. This mandates the automated application of static application security testing, dependency scanning and secrets detection as a standard. The framework also stipulates requirements for approvals in merge requests.

Technological Security

Endpoint Devices

Enterprise-grade endpoint security solutions are deployed throughout the Darktrace fleet, including coverage from an enterprise-wide Darktrace deployment. Desktops, laptops and mobile devices use mobile device management (MDM) solutions.

Configurations for endpoints are determined by the system owner. Further guidance is provided in the Configuration Management Policy.

Employees are responsible for keeping devices up to date with the latest approved OS version as outlined by the Security Team. Emergency updates are to be installed within 7 days of release.

Protection Against Malware

Endpoint detection and response (EDR) and anti-virus (AV) products are deployed on devices remotely using MDM. Malware and AV signatures are updated daily with definitions released by the vendor. Scans are run regularly and in real-time on devices. AV is configured to automatically quarantine or remove files detected. Tamper protection is enabled to prevent modification or removal of the EDR and AV. Alerts from EDR and AV are investigated by the Darktrace Internal Security Team and suspected infections dealt with under the Incident Management processes.

Information Backup

Darktrace operates a comprehensive backup program. A formally documented Backup Policy is maintained by the IT Group and Security Team. The Backup policy outlines the requirements for backing up all applicable internal information systems. Backups of critical information systems are performed daily.

Comprehensive backup measures are in place for cloud-based deployments of Darktrace products and services.

Logging

Information and event data is recorded from network, application, cloud, email and endpoint sources. Log data is protected against tampering. Access to the log server, collection server, anti-virus server and the internal Darktrace monitoring systems are highly restricted.

Monitoring

Darktrace's Internal Security Team monitors security events taken from anomalous

network, endpoint, cloud and email alerts and investigates these in real time. Access to the log server, collection server, anti-virus server and the internal Darktrace monitoring systems are highly restricted. Darktrace appliance aids attribution, including remote VPN users and administrator activities.

Networks Security

Darktrace leverages an enterprise-wide Darktrace deployment to protect sensitive information assets, which covers cloud-hosted systems, the Darktrace email environment, SaaS applications, internal networks and user endpoints. Darktrace operationally uses all key product capabilities - /NETWORK™, /ENDPOINT™, /IDENTITY™, /CLOUD™, /EMAIL™ and /Attack Surface Management™ - to defend its systems from cyberattack.

Web Filtering

Darktrace has applied preventative controls to ensure users are protected while using the internet. Known or suspected malicious websites, in addition to websites sharing illegal content are blocked by AV solutions. Anomalous connectivity in malicious endpoints is blocked in real-time by the Darktrace /NETWORK™ and /ENDPOINT™, capabilities will additionally detect and block anomalous uploads on websites.

Employees are provided guidance on the securely using the internet as part of biannual Security Awareness Training and is covered within the Acceptable Use & IT Security Policy.

Data Security

Classification and Labelling of Information

Darktrace utilises a classification system for internal information assets. Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. Disclosure of information classified at the lowest level represents insignificant harm to the business, while disclosure of information classified at the highest level may seriously impact the business or an individual. Information is stored, handled, transferred and disposed of in line with the classification level requirements. A list of information assets is kept with their assigned level of classification. A formally documented Data Classification Policy, applicable to all Darktrace employees, further outlines classification, labelling and handling requirements for internal information assets.

All unmarked documents and media are assumed to have the lowest classification. Auto-classification rules are applied to documents generated within, processed by, or saved to Microsoft 365 environments, in-line with the Data Classification Policy. All

documents with higher classifications are marked as such, either in the document header or footer. Where not possible to mark the document itself, the classification is present on the container or access route (e.g., as metadata, or a folder name).

All Darktrace employees receive regular training on data classification and handling requirements, as part of the mandatory bi-annual Security Awareness Training. Failure to comply with handling requirements may result in formal proceedings.

Data Leakage Prevention

Data leakage prevention solutions and controls are configured against the classification of documents and information assets, including access permissions, monitoring of activity on workstations, reclassification of documents, and internal and external sharing channels to prevent data from being improperly accessed, deleted or exfiltrated. Removable media and USB ports are blocked by default on all workstations.

Darktrace /EMAIL™, /NETWORK™, /IDENTITY™ and /ENDPOINT™ can help identify and block potential transfer or exfiltration of sensitive information.

Data Encryption

Data is encrypted both at rest and when transmitted over public networks. Only authorised, vetted personnel have access and there is a documented privacy policy for the protection of information transmitted, processed or maintained on behalf of the customer.

All corporate devices use disk encryption using native methods (FileVault 2 for MacOS, Native for iOS, BitLocker for Windows, LUKS for Linux) or VeraCrypt. Email is encrypted in transit using TLS encryption and will be encrypted in the email server hard drive. PDF file version higher than or equal to 1.6 are encrypted with AES. Microsoft Office documents (Excel, PowerPoint, Word) are encrypted using native methods in Office 2013 and above. ZIP files are encrypted using AES-128 or AES-256 with file names hidden.

Data is transmitted with TLS1.2+ (HTTPS, SMTPS, POPS etc), SSHv2, IPsec/DTLS with AES-128- GCM or higher encryption. Weaker ciphers from the available suite are removed. SMBv3 is encrypted with AES-CCM encryption. Further details are outlined in the internal Cryptographic Policy.

Key Management

Cryptographic keys have a fixed valid period, as defined within the Cryptographic Policy. Management of cryptographic keys for Cloud Master deployments is outsourced to the 3rd-party cloud provider's trusted key management solution.

Controlling Access to Customer Data

Access to systems housing customer data is based on least-privilege and need to know principles.

For Darktrace product offerings, the customer controls access to their data. On request from the customer, to provide contracted support services, limited assigned Darktrace employees will have access to customer data. Third parties or subcontractors do not have access to customer data.

Data Retention

The retention of records, including customer information is outlined in the Data Retention Policy. All applicable data and documentation held within the business, both physical and digital in nature is included in scope.

Digital and physical documents will be retained for the length of time required in accordance with legal, regulatory or contractual obligations. Where documentation is not required to be retained, it may be held for as long as the data owner deems necessary.

Data pertaining to client personal data and HR records is to be held and maintained in accordance with the Data Protection Act 2018. Data and documentation pertaining to Information security must be retained securely and indefinitely.

Data Deletion

A Data Destruction Policy is available and applies to all media and devices.

Darktrace only utilises approved destruction suppliers, as outlined in the Approved Supplier List. Certificates of destruction are provided for all retrieval and destruction actions carried out by the approved suppliers.

Hard drives containing sensitive information are wiped before re-use or disposal. If encrypted, deleting the partition is sufficient. Secure disposal procedure for all hard copy documentation, confidential waste, and HDD data. Destroyed to BS EN15713:2009 Standards.

On termination of the Agreement, Darktrace shall delete or return to customer all customer data in its and/or its sub-processors' possession or control, in accordance with the customer's written instructions. Customer cloud environments are decommissioned at end/termination of contract, with encryption keys deleted.

People Security

Prior to Employment

At least two professional references are taken, academic and professional qualifications are confirmed, and a passport check is completed to confirm identity. For all roles with access to key company or customer information, a criminal background check and an Experian Complete check are conducted, which includes a financial stability check. For US employees, SSN checks are performed in place of Experian Complete checks.

Onboarding

Upon hiring, new staff are assigned equipment and accesses based on their role. Access to internal systems and resources is granted to new hires on start date by IT. A security presentation is provided to all new joiners on induction.

Role Changes

Role changes are subject to the change control process. When changing roles, HR will update the HR system which will inform the IT department of a role change. Accounts are role based and will be automatically provisioned/revoked by IT systems.

Leavers

The leavers process is documented in the Exit Process policy. Upon receipt of a resignation letter or termination of contract by the company, the HR team will update the HR system with the users exit date. Management/HR decide whether the employee will work their notice period or leave immediately.

On exit date, IT will disable all relevant accounts they manage and arrange for removal of others via ACP1. All equipment is to be returned. Contracts contain provisions to withhold the value of the equipment from the final paycheck until returned.

Terms and Conditions of Employment

Employee contracts include strict non-disclosure agreements and enforce compliance with information security policies. The employee contract documents the employees ongoing obligation to non-disclosure and confidentiality post-termination.

Security Awareness and Training

An Acceptable Use & IT Security policy is issued in a welcome pack to all staff. A security

presentation outlining risks to Darktrace, and employee obligations is discussed at all new joiner inductions. Presentations on security are included at major internal gathering events. High priority security alerts are emailed to all staff.

Interactive biannual training sessions are hosted on a dedicated training platform. Training material is based on:

a) current and emerging threats within the wider security landscape, ensuring our employees are made aware of novel threats.

b) trends seen throughout the organisation, allowing us to further strengthen our baseline security posture.

c) current and emerging regulatory requirements.

In addition to general information security training, department-specific training is conducted where applicable (e.g., software development). Completion is mandatory for all staff and is tracked and enforced by the Security team. Failure to complete the training may result in formal proceedings.

The Security Team is accessible to all Darktrace staff, with multiple dedicated communication channels (mobile contact, email inbox, Teams), as well as a physical presence in select offices.

Disciplinary Process

A Disciplinary and Capability procedure is formally documented in the Staff Handbook and included in the employee contract.

Darktrace may follow formal proceedings for instances of non-conformance with any Information Security, Privacy, HR or Legal policies and procedures.

Physical Security

Physical Access

Internal office access restrictions are set with the use of electronic HID cards with photographic identification. Physical security practices include reception attendance during work hours and visitor access being limited to main reception areas, unless escorted by an authorised member of staff. Each user is provisioned a specific access card which should be returned upon leaving the organisation. Anti-tailgating controls are provided in some offices. Visitors to offices should follow the Visitor Access Policy and follow requirements around supervision if applicable.

Secure Area Access

For locations containing critical Darktrace operating infrastructure, including offices

within the scope of ISO 27001, access control systems are operated and managed by the Security Team. These systems are continuously monitored for unauthorised access. Sensitive internal zone access is determined by role and is subject to a privileged access request, in line with the Access Control Policy.

Perimeter Security and CCTV

CCTV and PIR systems cover all entrances, internal corridors and secure areas. The retention period of the associated data is approximately 30-90 days, depending on location. All main office entrances are accessed through a shared building lobby with manned reception. For all non-critical offices, perimeter security and CCTV systems are operated and monitored by building management teams.

Loading and Delivery

All build, loading and delivery locations (Cambridge, Dublin and The Hague) are covered by robust, technical access control systems and CCTV. CCTV covers external and internal movements in full. Deliveries for all locations are taken, logged and screened by onsite security or building management. Larger deliveries for non-build locations are managed by the building management teams. These locations are all covered by access control and CCTV.

Environmental Threats

Layered entry defences are used to protect from environmental threats. Headquarters and data centres are not located in a flood plain or on a flight path. Fire detection and suppression equipment, and leak detection systems, are in place within these locations.

Clear Desk and Clear Screen

Darktrace maintains an internal Clean Desk Clear Screen Policy designed to outline information protection requirements for Darktrace users. Users must guard against shoulder-surfing, minimise the production of printed materials, and ensure screen-locking is automated after a short period of inactivity.

It is best practice to avoid printing physical documentation, especially when involving Personal Identifiable Information (PII). Where unavoidable, it must be kept in lockable storage. Before printing and storing documentation make sure the following are present: secure and lockable storage, cross-cut shredder is available.

Printers must be procured and issued by the IT Department unless already approved by the Security Team or IT Department.

Supplier Security

Supplier Onboarding

Business owners identify and negotiate the services provided by suppliers. The Security Team should be consulted for all new suppliers to assess the criticality level of the supplier. The criticality level is based on the importance of the service as part of Darktrace's business operations combined with the potential business impact of a breach, impacting Darktrace's reputation, valuation and customers.

The Security Team will identify vendor risk management and assurance requirements, based on the system criticality. Further detail is outlined in the Approved Supplier Policy.

Information Security Requirements for Suppliers

Suppliers must meet Darktrace's pre-defined information security requirements. The Security Team will perform a comprehensive review of the supplier's security controls, prior to onboarding. Information security provisions must be established and agreed with each supplier, based on the type of supplier relationship. If a supplier fails to meet Darktrace's requirements, the supplier will be offboarded.

Onboarding Cloud Services

All new systems, vendors or suppliers which are cloud-hosted will undergo a cloud-centric vendor risk management process. The Security Team shall certify that security, data privacy and governance, and all other requirements around the protection of Darktrace information are adequately addressed by the cloud service provider.

Senior leaders in Security, IT and Development operate the Systems Review Board to formally approve new cloud services. Security and IT teams will be embedded within system implementation projects where applicable. Further requirements are outlined in the SaaS Data Security Policy.

Supplier Risk Management

The onboarding process may enumerate information security risk, which will be treated in the information security governance program. The Security Team will periodically review the risks posed, based on the assigned criticality of the supplier and assessed risk. Senior approval may be required is a system is assessed to pose an increased level of risk.

Security Incident Response

Incident Management

Darktrace maintains comprehensive incident reporting and response guidelines, establishing a consistent response and management to suspected and authentic information security incidents. An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Darktrace's main objective is to protect sensitive customer, prospect, business and confidential information according to legal, client and procedural requirements.

A formal incident report is written to determine the root cause. This is then reviewed to determine corrective and preventative actions. Where appropriate, lessons learned will be presented in bi-annual security training, or department-specific training.

Roles and Responsibilities

Incidents are raised to the Security Team, following Incident Reporting and Security Event Contact guidelines. The Security Team is the main point of escalation for the management and remediation of information security incidents. Additional roles and responsibilities have been identified, with internal stakeholders having been made aware of their incident management responsibilities.

Evidence is collected, analysed and stored securely by the Security Team, and accessed only be investigators. All investigators are independent of the incident itself.

Privacy Breach Procedure

Upon identification of a potential privacy breach, involving Personally Identifiable Information (PII), the Security Team will notify the Privacy Team and Data Protection Officer (DPO). Privacy assessment tooling is available and can be used to identify reporting requirements to either the affected individual or relevant privacy regulator. Should reporting be required, the Privacy team will lead the communications plan with the relevant parties.

Darktrace has identified the relevant supervisory authorities and is responsible for reporting a personal data breach to the respective authority. Darktrace will ensure all available controls are applied to personal data to safeguard the storage, transmission and processing of such data.

Notification

The business impact of an event is assessed by the relevant teams, and if customer is

plausibly at risk, customers are notified without undue delay. The Executive Team are notified within 24 hours of an information security incident.

Training and Testing

The Security Team conducts incident response tabletop exercises throughout the year. Select departments, key members of upper-management, and the executive team participate in attack simulations, ensuring that the incident response members are aware of, roles and responsibilities, response priorities, order of events, communication requirements and the security tools available at the team's disposal.

Incident response procedures are tested and validated, with findings being addressed by both the Security Team and relevant department(s). Findings identified during tabletop exercises are captured by the Security Team, and are logged as opportunities for improvement. Findings will be addressed by the Security Team and will be used to continually improve incident response management procedures.

Learning from Security Incidents

An incident register is maintained by the Security Team which highlights learning points identified in the post-incident assessment. The Incident Register is reviewed by the Security Management Team to identify key issues and trends and support the content of future security awareness training. Learning points and action items from the post-incident assessment are regularly reviewed to ensure continuous improvement.

Threat Intelligence and Threat Hunting

Darktrace has formally defined a Threat Intelligence function within the Security Team. Darktrace utilises multiple threat intelligence feeds to act upon external threats, both internally and for customers. This includes news / open-source intelligence feeds, technical indicator of compromise system integrations and email communications from threat intelligence sources. These feeds support operational actions in the security team (e.g., threat hunting, website blacklisting), as well as informing strategic business risk management activities (e.g., geopolitical changes to operating environment).

Outputs from routine Threat Intelligence and Threat Hunting exercises are presented to Security Management and relevant stakeholders throughout the organisation.

Privacy

Privacy Statement

Darktrace is committed to protecting and respecting customer and employee privacy. Darktrace collects, uses and keeps information in compliance with the UK Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the General Data Protection Regulation (Regulation (EU)2016/679) ("GDPR"), the California Consumer Protection Act (CCPA) as amended by The California Privacy Rights Act (CPRA), the Colorado Privacy Act (CPA), the Virginia Consumer Data Protection Act (CDPA), the Connecticut Data Privacy Act (CTDPA), the Utah Consumer Privacy Act (UCPA) and all relevant regulations.

Darktrace will not sell any data captured as part of a customer's use of Darktrace's products or services.

International Data Transfers

Where customer data originates in the EEA or the UK, Darktrace will not transfer such customer data to the third country, without the prior written consent of the customer and not without procuring provision of adequate safeguards (as defined by the relevant authority) in accordance with the applicable data protection laws.

GDPR

Under the GDPR and DPA18, Darktrace is obliged to appoint a Data Protection Officer (DPO). Darktrace has appointed this role to Iain Pye, privacy@darktrace.com.

Compliance and Risk Management

Darktrace makes a commitment to our customers, partners, employees and shareholders to ensure that our product offerings, and organisation, meets international industry standards for information security, data privacy and compliance.

Upon a customer's written request, and subject to appropriate confidentiality obligations, Darktrace will make available to the customer: a) a copy of the current certificate in relation to the ISO 27001, ISO 27018 and Cyber Essentials certificate; and b) the Statement of Applicability, demonstrating the implementation of all applicable controls.

ISO/IEC 27001

ISO 27001 is a globally recognised information security standard that outlines best practice for operating a successful information security management system. To

achieve and maintain this certification, regular audits are required, alongside a formal recertification every three years. The certificate can be provided upon request and holds the number IS 771724.

Darktrace is applicable to 92 out of the 93 Annex A controls outlined in ISO 27001:2022. Darktrace does not outsource the development of any products or internal systems, and thus control 8.30 'Outsourced development' is not deemed applicable.

ISO/IEC 27018

ISO 27018 is a standard that outlines critical security controls to protect personally identifiable information (PII) in public cloud environments. For this certification, all cloud-hosted Darktrace products are in scope. To achieve and retain this certification, Darktrace is audited bi-annually by an independent third-party. The certificate number is PII 771726.

Cyber Essentials

Darktrace also maintains the Cyber Essentials certification. This is a UK-backed framework supported by the National Cyber Security Centre (NCSC). The framework outlines a baseline set of controls to protect organisations from cyber-attack. The certificate can be provided upon request.

Auditing

Darktrace's ISO 27001 and ISO 27018 certifications require routine audits from our issuing body in order to retain the certifications. In addition to this, internal audits are conducted throughout the year by an external assessor, ensuring both the organisation, and our products, meet our stringent requirements for security.

The outputs from audits are used, in part, to drive the continual improvement cycle, helping further strengthen the Information Security Management Systems (ISMS).

Enterprise Risk Management

A risk management program has been developed to manage information security risk throughout the business. The risk management program is within the scope of Darktrace's ISO 27001 certification.

Darktrace has appointed a Head of Enterprise Risk Management, designated to oversee the risk management program. Risk assessments are performed on an annual basis. Risks are recorded within a risk register. Darktrace's risk assessment methodology and threshold are documented within Risk Management Policy. Darktrace subscribes to the ISO 31000:2009 risk process.

Legal and Contractual Requirements

All relevant statutory, regulatory, and contractual requirements have been identified. Darktrace's approach to meet these requirements has been explicitly defined, documented, and is kept up to date for each information system.

Exceptions

In extreme cases, there may be a need for an exclusion from a policy within the Information Security Management System (ISMS). Any requests for exclusions must follow the ISMS Exceptions Policy requirements and will need to be approved by the Global CISO or another appropriate member of the Security Management Team.

All exclusions must have a business reason and timeframe for review. Permanent exclusions will not be approved. Failure to obtain exception approval will be considered a breach of the ISMS Exceptions Policy. Formal proceedings may be followed for employees who do not adhere to the requirements outlined in the policy. A register of all exclusions will be maintained by the Security Team and reviewed at least quarterly.

Dispensations

In case of any further dispensations or deviations from this document please contact the document owner.