Appendix 3 - Data Processing Addendum

This Data Processing Addendum is supplementary to and shall be construed in accordance with the Darktrace Master Services Agreement available at https://darktrace.com/legal/master-services-agreement (the "**Agreement**").

1. Definitions

Unless otherwise defined in the Agreement, all capitalised terms in this Data Processing Addendum ("**DPA**"), shall have the following meanings:

"**Authority**" means for Personal Data originating in the:

a) EEA, the European Commission; and

b) UK, the Information Commissioner's Office,

"**Customer Data**" means the Personal Data that is shared by the Customer with Darktrace in performance of the Services;

"**Controller**" has the meaning given to it in the GDPR Laws;

"**Controller-to-Processor Clauses (2010)**" means the standard contractual clauses for the transfer of Personal Data to Processors established in Third Countries set out in the European Commission's Decision 2010/87/EU of 5 February 2010 and at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 and which together with its appendices included in Schedule 5 form a part of this DPA;

"**Darktrace Affiliates**" means all persons and entities directly or indirectly controlling, controlled by or under common control with Darktrace, where control may be by management authority, equity interest or otherwise;

"**Data Protection Impact Assessment**" has the meaning given to it in the GDPR Laws;

"**Data Protection Laws**" means all data protection and privacy laws, including guidance issued by any applicable data protection authority, applicable to any Personal Data, as may be amended or replaced from time to time, including without limitation:

a) in the European Union, the General Data Protection Regulation 2016/679 (the "**EU GDPR**") and the Privacy and Electronic Communications Directive 2002/58/EC (as the same may be superseded by the Regulation on Privacy and Electronic Communications);

b) in the UK, the UK General Data Protection Regulation 2016/679, as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 (the "**UK GDPR**"), the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 a; and

c) in the United States of America the California Consumer Privacy Act of 2018.

"**Data Subject**" has the meaning given to it in the GDPR Laws;

"**Documented Instructions"** has the meaning given to it in paragraph 3 of this DPA;

"**EEA**" means the European Economic Area;

"**EU Processor-to-Processor Clauses**" means the standard contractual clauses between processors for data transfers to Third Countries, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://darktrace.com/legal/customer-model-clauses;

"**EU Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for data transfers to Third Countries, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://darktrace.com/legal/customer-model-clauses;

"**GDPR Laws**" means the EU GDPR and the UK GDPR collectively;

"Information Security Policy" means the information security policy contained in **Error! Reference source not found.**;

"**Personal Data**" has the meaning given to it in the GDPR Laws;

"**Personal Data Breach**" means any breach of security or other action or inaction leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data by Darktrace, its affiliates, sub-processors, or any other identified or unidentified third party;

"**Processor**" has the meaning given to it in the GDPR Laws;

"**Standard Contractual Clauses**" means the EU Processor-to-Processor Clauses, EU Controller-to-Processor Clauses and the Controller-to-

Processor Clauses (2010);

"**Third Country**" means in respect of Personal Data originating in the:

a) EEA, a country outside of the EEA not recognised by the European Commission as providing an adequate level of protection for Personal Data (as described in the EU GDPR); and
b) UK, a country outside the UK not recognised by the Information Commissioner's Office as providing an adequate level of protection for Personal Data (as described in the UK GDPR).

2. Data Processing

2.1 Scope and Roles

This DPA applies when Darktrace processes Customer Data under the Agreement. In this context, Customer is the Controller and Darktrace is the Processor. Each Party agrees that it will comply with all Data Protection Laws in exercising its rights and performing its obligations under this Agreement, as such laws apply to a Controller and Processor respectively.

2.2 Details of the Processing

(a) **Subject matter:** The subject matter of the data processing under this DPA is Customer Data.
(b) **Duration:** Customer Data shall be processed under this DPA for the Term.
(c) **Nature and purpose:** Darktrace will process Customer Data for the purpose of providing the Services to Customer. [In the event that Customer has purchased that part of the Offering referred to as Antigena Email, the data protection provisions of the Antigena Email Schedule shall apply and be incorporated into this DPA].
(d) **Categories of Data Subject:** The categories of Data Subject, whose Perssonal Data may be processed by Darktrace as Customer Data include Customer's clients and prospects; Customer's officers and directors; Customer's employees, temporary workers, agents and volunteers; independent contractors engaged by the Customer; Customer's suppliers and vendors; advisors, consultants and other professional experts engaged by the Customer; and any other categories of Personal Data that may be contained in the Customer Data.
(e) **Types of Personal Data:** The types of Personal Data that Darktrace may process include: names; phone numbers; addresses; and any other types of Personal Data that may be contained in the Customer Data.

3. Instructions

3.1 The Parties agree that this DPA and the Agreement (including any instructions provided by Customer to Darktrace required for or related to the performance of the Services) constitute Customer's documented instructions regarding Darktrace's processing of Customer Data ("**Documented Instructions**"). Darktrace will only process Customer Data in accordance with Documented Instructions unless required to do so by applicable law, in which case Darktrace will, to the extent legally permissible, inform Customer of that legal requirement before processing. Darktrace shall promptly inform Customer if, in Darktrace's opinion, an instruction from Customer infringes the Data Protection Laws.

3.2 If Customer Documented Instructions require Darktrace to perform actions that go beyond its obligations under this DPA or the scope of work for the Services set out in the Agreement, Darktrace shall inform the Customer and require the Customer to provide different Documented Instructions, the carrying out of which will fall within the scope of the Services or within the scope of Darktrace's obligations under this DPA.

4. Confidentiality

4.1 Darktrace will take reasonable steps to ensure the reliability of any persons authorised to process any Customer Data and shall ensure that all such persons have committed themselves to confidentiality.

5. Security

5.1 Considering the nature, scope, context and purposes of processing, the Darktrace has implemented and will maintain for the Term, the administrative, physical, technical and organisational measures as set out in the Information Security Policy to protect any Customer Data accessed or processed by it against unauthorised or unlawful processing or accidental loss, destruction, damage or disclosure.

5.2 The Parties agree that for the purposes of processing Customer Data under this DPA and the Agreement, the measures contained within the Information Security Policy are appropriate, given the nature of the data to be processed and the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction, disclosure, access or damage.

5.3 Darktrace has been certified as operating an Information Security Management System which complies with the requirements of in ISO 27001 (ISO/IEC 27001:2013) and ISO 27018 (ISO/IEC 27001:2019) and Darktrace will continue to maintain such certifications (or equivalent) for the duration of the Term.

6. Sub-Processing

6.1 Save as expressed in paragraph 6.2, Darktrace shall not without the prior written consent of Customer, engage any sub-processors for the processing of Customer Data under this Agreement.

6.2 Customer consents to and authorises Cloud Provider and Darktrace's Affiliates to act as sub-processors for Darktrace in the provision of the Services and on terms materially equivalent to those contained in this DPA. Darktrace shall be fully liable for any breach by the sub-processors of any of the obligations contained in this DPA .

7. Cross-Border Transfers

7.1 Save as expressed in paragraph 7.1, if Customer Data originates in the EEA or the UK, Darktrace will not transfer such Customer Data to a Third Country, without the prior written consent of Customer and not without procuring provision of adequate safeguards (as defined by relevant Authority from time to time) in accordance with applicable Data Protection Laws.

7.2 Customer Data may be hosted by the Cloud Provider in the Hosted Location specified in the Product Order Form. Customer acknowledges and consents to the processing of Customer Data outside of the EEA and UK, solely and to the extent necessary for Darktrace to provide the Services and for which purposes the relevant Standard Contractual Clauses shall apply.

7.3 When Customer is acting as a controller and transfers Customer Data originating in the:

(a) EEA, to a Processor located in a Third Country, the EU Controller-to-Processor Clauses will apply; and

(b) UK, to a Processor located in a Third Country, Controller-to-Processor Clauses (2010) will apply.

7.4 When Darktrace, its affiliates, or any other identified or unidentified third party is acting as a Processor and transfers Customer Data originating in the:

(a) EEA, to a Processor located in a Third Country, the EU Processor-to-Processor Clauses will apply; and

(b) UK, to a Processor located in a Third Country, the Controller-to-Processor Clauses (2010) will apply.

7.5 The Parties agree that Darktrace, may at its sole discretion, update and or entirely replace paragraphs (a) and (a) of this DPA, which concern transfers of Customer Data originating from the UK to a Third Country, if the Information Commissioner's Office provides an alternative or replacement recognised compliance standard for such transfers in accordance with the UK GDPR, to that already stated in this DPA. Darktrace will provide notice of such change in writing to Customer.

8. Data Subject Requests and Assistance

8.1 Darktrace shall use reasonable efforts to promptly notify Customer if it receives:

(a) a request from a Data Subject to have access to that person’s Personal Data; or

(b) a complaint or request relating to Customer’s obligations under the Data Protection Laws; or

(c) any other communication relating directly or indirectly to the processing of any Personal Data in connection with the Agreement.

8.2 Considering the nature of processing and the information available to the Darktrace, Darktrace will provide reasonable support to Customer in:

(a) complying with any legally mandated request for access to or correction of any Personal Data by a data subject under Chapter III of each of the GDPR Laws (and where such request is submitted to Darktrace, Darktrace will promptly notify Customer of it);

(b) responding to requests or demands made to Customer by any court or governmental authority responsible for enforcing the Data Protection Laws; and

(c) in its preparation of a Data Protection Impact Assessment.

9. Personal Data Breach

9.1 aware of a Personal Data Breach it will inform Customer without undue delay, of becoming aware of the same and take reasonable steps to mitigate the effects and to minimise any damages resulting from such breach.

9.2 In the event of a Personal Data Breach, Darktrace (to the extent reasonably possible), will provide the following information to Customer:

(a) a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of the relevant Processor's data protection officer or another contact point where more information can be obtained;

(c) a description of the likely consequences of the incident; and

(d) a description of the measures taken and / or proposed to be taken by the relevant Processor to address the incident including, where appropriate, measures to mitigate possible adverse effects.

10. Audit.

10.1 Darktrace agrees to maintain its ISO 27001 and ISO 27018 certifications for the duration of the Term. Darktrace will use an external auditor to verify that its security measures meet ISO 27001 and ISO 27018 standards in accordance with the ISO certification process. On Customer's written request, and subject to appropriate confidentiality obligations, Darktrace will make available to Customer:

(a) a copy of the current certificate in relation to the ISO 27001 and ISO 27018 certification; and

(b) any information reasonably requested by Customer concerning Darktrace's processing of Customer Data under the Agreement and this DPA.

10.2 Other than in the context of investigating a Personal Data Breach involving Customer Data, Customer agrees to exercise any right it may have to conduct an audit or inspection under Data Protection Laws (or the Standard Contractual Clauses, if applicable) by requesting the information outlined in paragraph 10.1.

11. Data Return and Destruction

11.1 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 Customer's written instructions.

SCHEDULE 1: DARKTRACE INFORMATION SECURITY POLICY

DARKTRACE

INFORMATION SECURITY POLICY

Table of Contents

1. 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. This document and all associated works are copyright © Darktrace 2022 unless otherwise stated. This document is not for distribution without the express written permission of the Darktrace document approver.

Issue Control			
Document Reference		**Project Number**	
Issue	3.0	**Date**	15/07/2022
Classification	DTL0	**Author**	Security Compliance Lead
Document Title	Information Security Policy		
Approved by	Deputy CISO		
Released by	Deputy CISO		

Owner Details	
Name	
Office/Region	Cambridge

Revision History			
Issue	**Date**	**Author**	**Comments**
3.0	15/07/2022		Annual revision

Distribution List			
Name	**Title**	**Company**	**Contact Info.**

2. 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 at Darktrace.

3. 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 Darktrace Plc.

4. ISMS

The Information Security Management System (ISMS) ensures the confidentiality, integrity and availability of all information at Darktrace Plc and its affiliates (“Darktrace”). This is achieved through policies, procedures and controls within the ISMS.

To give the ISMS purpose and direction, measurable information security objectives have been agreed based upon a risk assessment and our overall business strategy.

5. Objectives

Darktrace’s ultimate security goal is to:

Protect Darktrace business and customer systems, managing risk across the operational estate, avoiding cyber disruption that would have an adverse impact to our customers, employees or shareholders.

Darktrace intends to achieve this goal with security objectives that are outlined in the OBJ1 Security Objectives document. Management gives complete approval and commitment to this policy to satisfy requirements related to information security, to comply with applicable PII protection legislation and to adhere to contractual terms. Management is committed to the continual improvement of the ISMS.

Poppy Gustafsson

Poppy Gustafsson
CEO
Darktrace Holdings Ltd
19th July 2022

6. Overview

As a cyber security company, the security of Darktrace and its customer information is paramount. It is essential that all parties; Darktrace employees, customers, suppliers and partners play their part in maintaining the Confidentiality, Integrity and Availability of information by upholding strong information security standards.

7. Information Security Certifications

ISO/IEC 27001
ISO 27001 is one of the most well-known, significant, and globally respected information security certifications. In order to achieve and retain this certification, regular audits are required, alongside a formal recertification every three years. Our certificate can be provided upon request and holds the number IS 645114.

ISO/IEC 27018
ISO 27018 is a security standard part of the ISO 27000 family of standards. It was the first international standard about the privacy in cloud computing services which was promoted by the industry. The standard helps cloud service providers who process Personally Identifiable Information (PII) to assess risk and implement controls for protecting PII. In order to achieve and retain this certification, we are audited bi-annually by an independent third-party against the standard.

Cyber Essentials
Darktrace also maintains the UK's Cyber Essentials certification. This is required as a baseline by all companies doing business with UK government entities. Our certificate can be provided upon request.

8. Access Control

Access to the organisation's network is limited to prevent unauthorised activity and unintended consequences.

Network Segregation
Darktrace utilises physical and logical segregation of networks. Most significantly, the core software development network is physically separate to all other internal networks. Guest wireless is physically separate to the corporate wireless network.

Remote Access
Darktrace operates a zero-trust networking solution for the majority of its end users. The zero-trust solution requires MFA and can route only to authorized applications.

Unauthorized Access

Devices are restricted from joining internal networks without authorisation. Antigena Network automatically denies any unauthorised devices that try to join internal networks. Wi-Fi connection details will not be shared without authorisation from the Security Team.

Visitor Access

Guests, visitors and third parties must not use the company's corporate Wi-Fi and must follow the visitor procedure. They may connect to one of the 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 the Server Room and must have their physical access limited appropriately to their work requirements.

Access Requests

In order to maintain an audit trail of system access, access requests are submitted to the IT Support Team via the helpdesk ticketing system. The requestor's job function as described by the HR department and their Line Manager are reviewed to ensure that the requested access is relevant and acceptable.

Access Authorisation

The IT Group has overall governance of access control within the company. Department managers are responsible for determining the access levels required by their staff. The Change Control managers, along with support from the Security Team, will evaluate all requests and authorisations to determine what access is required.

Privileged Access

The use of privileged accounts (admin/root) will be limited, operating on need to know and least-privilege principles. 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 admin roles.

Access Review

Access to systems will be regularly reviewed, to ensure that users are still authorised to access each system. The Security Team will request 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.

Logging and Monitoring

User activity is logged and routinely monitored for the purposes of error detection and security.

Passwords

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 10 characters.

9. SDLC

All products/services developed by Darktrace are designed with the philosophy of security by design. Testing is carried out at all stages of development.

Open-Source Code Policy

All open-source usage, whether the open-source is used internally, as part of the Company's products, or as part of a web service, is subject to review through the OSS approval process. In order to help Darktrace achieve its OSS objectives, Darktrace has appointed the position of OSS Compliance Officer (OSSCO). The OSSCO will be the first line of support for the development community within the Company on questions around OSS.

Vulnerability Management

The Dev/Ops team will keep themselves informed of security notifications for any underlying libraries and platforms and will push out patches as part of the regular product updates. Python and NPM security tools are also used for automated auditing of security vulnerabilities.

Penetration Test Methodology

A full penetration test by a suitably competent specialist is conducted before each major version release or annually, whichever occurs first. Such a test will include vulnerability scanning and skilled manual attacks at all levels of the TCP/IP stack including the Web application and SSH server. Tests are conducted initially without a valid credential and then with a credential for the Web application.

Results and Remediation

Results are presented in descending order of severity using a recognised, industry standard scoring system such as CVSS. Findings of a severity of CRITICAL or HIGH (>= 7) will be fixed and the complete test will be repeated until no such findings remain before the version is released to customers. MEDIUM (>= 4) findings will be addressed by an automatic update deployed to customers within 30 days. LOW (< 4) findings will be addressed before the next major release.

10. Physical Security

Loading and Delivery

The main delivery route for build locations (Cambridge and Dublin) is managed by access control systems, and CCTV covers the building perimeter on the internal approach. This has visibility over all external and internal movements. Packages being moved internally are covered at all times by CCTV and are not left unattended with the external door open. General deliveries for all locations are taken and screened by onsite security / building management. Under no circumstances are general delivery drivers allowed to enter the main building through the building's delivery route.

Larger deliveries for non-build locations such as London, San Francisco, Singapore, Los Angeles, New York, Reston and Paris are managed on prior notice to the building management teams. These locations are all covered by access control and CCTV by the building management team in the respective location.

Perimeter Security
CCTV and PIR systems cover all entrances, internal corridors and secure areas. The retention period of the associated data is approximately 30 days. All Office entrances are accessed through a shared building lobby with manned reception. Internal office access restrictions are set with the use of electronic HID cards with photographic identification. All locations containing Darktrace critical infrastructure, and restricted and secure areas, utilise access control systems operated and managed by the internal security team. Internal zone access is determined by role.

For all locations with non-critical infrastructure, access control and CCTV systems are operated and monitored by the respective building management teams.

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.

11. Asset Management

Inventory of Assets
A full asset inventory database is maintained by the IT/Security Team for all devices with 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.

Return of Assets
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.

12. Information Classification

Classification of Information
Darktrace utilises a classification system for internal information. 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.

Labelling of Information
All unmarked documents and media are assumed to have the lowest classification. 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).

13. Operations Security

Operational Procedures

All changes are risk-assessed and recorded within the ticketing system. Significant changes require recorded approval by a restricted list of approvers. Capacity management, where limitations exist, is tracked. Only late stage testing occurs on a staging server in operational environments. Operational networks are logically segregated.

Protection from Nefarious Threats

Darktrace utilises its own proprietary leading AI security technology, Enterprise Immune System (EIS) and Antigena Email (AGE), to learn normal 'patterns of life' in our internal and production environments to discover unpredictable cyber-threats, while delivering complete visibility across our dynamic workforce — from cloud and collaboration tools to endpoints. Darktrace's world-class SOC provides 24/7 monitoring and mitigation. Network activity is continuously monitored by the Darktrace EIS with full Antigena module enablement. AGE is also in place to monitor exchange traffic. Enterprise-grade endpoint security solutions are deployed throughout the Darktrace fleet. Cloud environments are monitored through security modules for SaaS and Web proxy filtering is in place.

Only approved software may be installed. Normal users do not have local administrative permissions, roles that require escalated privileges are monitored and their use is limited for specific approved actions only.

Logging and Monitoring

Network traffic logs are collected and passed into a Darktrace appliance. Security alerts from anomalous network events are investigated in real time. Security events and incidents are recorded. Clock synchronisation is achieved via NTP to internal servers. Access to the log server, collection server, anti-virus server and the internal Darktrace appliances is highly restricted. Darktrace appliance aids attribution, including remote VPN users and administrator activities. Log data is protected against tampering.

Control of Operational Software

Only software on the company's approved software list may be installed on laptops, workstations and phones. A formal change control procedure is in place. Access to administrative credentials is restricted and devices are built to a standard specification. Development and Operations teams manage instances of customised or in-house software.

Internal Technical Vulnerability Management

Auto-updates are enabled wherever possible. Important updates for other devices are rolled out as soon as possible and general updates are applied at least monthly. Websites are protected by anti-DDoS hosts. Vulnerability scanning of internal and external infrastructure is performed on a monthly basis. Findings from the vulnerability scans with a CVSS severity of CRITICAL or HIGH (>= 7) will be fixed within 7 days. MEDIUM (>= 4) findings will be addressed by an automatic update within 30 days. LOW (< 4) findings will be addressed as part of the monthly patch cycle.

14. Incident Management

Responsibilities and Procedures

Incidents are raised to the Security Team. The business impact of the incident is assessed and if customer data is at risk, customers are notified within 24 hours. Evidence is collected and stored securely by the Security Team and accessed only by investigators. All investigators are independent of the incident itself. A formal incident report is written to determine the root cause, this is then reviewed to determine corrective or preventative actions.

Learning from Security Incidents

An incident, event and non-conformity (IENC) log is kept and used in forum meetings with senior management to identify key issues and trends. This is also used to determine the content of future security awareness training.

15. Data Protection and Security

Data is encrypted both at rest and when transmitted over public networks. Only authorized, 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.

Acceptable File Encryption

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 using Darktrace certificates within an email client. 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.

Acceptable Transmission Encryption

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.

Appliance Encryption

Darktrace appliances are encrypted via LUKS with keys stored on TPM using a 256-bit AES cipher and sha256 for key derivation. All hard drives have full disk encryption, except the boot hard drive, which contains a small unencrypted boot partition for starting up the appliance.

Call-Home Functionality

The Darktrace appliance makes an encrypted outbound SSH connection to Darktrace HQ. This is fully under the control of the customer and can easily be disabled within the appliance's interface. Both sides of the connection enforce the correct pre-configured keys, which are unique to each customer. The connection is encrypted using the AES-128 CTR cipher. Only connection attempts from the customer's nominated IP ranges are permitted. The connection terminates in a Call Home host that is dedicated solely to the customer. All logins and activity are logged and monitored, and authentication is multi-factor. The call home host and all connections to it are monitored 24/7 by the Enterprise Immune System, as well as other security controls.

Data Destruction
Secure disposal procedure for all hard copy documentation, confidential waste, and HDD data. Destroyed to BS EN15713:2009 Standards. Customer cloud environments are decommissioned at end/termination of contract, encryption keys are deleted.

16. Web Application Security

Transport Layer Security (TLS)
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 v1.2 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. The following *should* be disabled: CBC modes, SHA1, 3DES.

Certificates
All external-facing web applications use an external trusted certificate authority. Sites that were live before 1 May 2018 may use RSA keys of at least 2048 bits, signed with SHA-256 or better hashes. New sites, released on or after 1 May 2018 will use ECDSA certificates, with optional additional legacy support for RSA.

Testing and Remediation
External-facing sites are regularly tested by Qualys SSL Labs and must get an A- or better grade. If the site fails to achieve the required grade, fixes are prioritised in order to obtain the required grade within 10 working days. Regular scanning is performed by ZAP and vulnerabilities scored according to CVSS. Remediation timescales for these findings are the same as those previously defined in the Product Testing section.

Authentication
Where required, new sites will avoid the need to create new credentials and should rely on existing identities or Single Sign-On (SSO) mechanisms. External-facing sites additionally require the use of one-time codes (TOTP 2FA) as provided by e.g., DUO mobile app.

Content
The web sites are designed to avoid the OWASP Top 10 vulnerabilities. In particular, 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 order to support the CSP header restrictions.

17. Human Resources 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.

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.

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
The 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 quarterly training sessions are hosted on the company Intranet, where completion is mandatory for all staff and is tracked and enforced by the Security team.

Disciplinary Process
A Disciplinary and Capability procedure is formally documented in the Staff Handbook and included in the employee contract. A formal incident response process exists and has been communicated to all staff.

18. Business Continuity and Disaster Recovery Planning

Business Continuity and Disaster Recovery Planning
A plan has been developed to provide continuity in the event of a long-term total effective loss of the network infrastructure, communications services, and/or working locations. The BC plan is updated and re-approved annually.

Service Recovery
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 senior management.

Business Continuity and Disaster Recovery Testing
The BC and DR plan are tested annually. Testing is routinely conducted throughout the year to maximise testing value and to identify remediation actions. Testing can include dry runs, tabletop exercises or full, live tests. Any remediations are identified, consolidated, logged and addressed in the subsequent tests.

Backup Policy
The Backup policy outlines the procedures and frequency of backup for critical information systems. Backups of critical information systems are performed Daily. Testing of backups is performed dependent on the information system which is outlined in the backup policy.

19. Cloud Security

Onboarding Cloud Services
Use of cloud computing services for Darktrace work purposes must be formally assessed by the Security Team. Cloud computing services providers are classed as a supplier and therefore must be reviewed, within the vendor risk management program, as per their assessed criticality and risk. The Security Team will certify that security, privacy and all other security requirements will be adequately addressed by the cloud computing service provider. Any risks or security control deficiencies identified should be addressed with the cloud service provider through the appointed Darktrace services/contract owner.

Cloud Based Deployments

Cloud based deployments of Darktrace products, such as AGE or Cloud-Masters, utilise hosted datacentres provided by Azure or Amazon AWS. Azure and Amazon AWS are a sub-processor of Darktrace. Customers can choose specific regions for Darktrace cloud services to be deployed in. This is covered in depth within our Master Hosted Terms.

20. Supplier Management

Business owners negotiate and approve the services provided by suppliers. The Security team should be consulted for all new suppliers to assess the criticality level. 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. New suppliers that may handle Darktrace data (e.g., Payroll providers) must meet the security criteria based upon their criticality level and should be flagged immediately to the Security team for inclusion in the approved supplier list. All suppliers identified as medium criticality and above should be identified and included within the vendor risk management platform.

Darktrace utilises the vendor risk management platform to actively manage information security risks to the business posed by suppliers. During the due diligence stage of vendor onboarding, once the criticality level has been identified, the Security team will utilise security questionnaires to ascertain the information security maturity of the supplier. Any significant risks are treated. Thereafter, the Security team will periodically review the risks posed, based on the assigned criticality of the supplier and assessed risk.

21. 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. An individual is 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 the Risk Management Policy. Darktrace subscribes to the ISO31000: 2009 Risk Process.

22. Data Privacy

A Data Privacy Program is implemented which ensures that employee, customer and third party personal data is secured in line with Personal Data regulations and laws in the countries, and regions, that Darktrace operates within. Darktrace is a Data Controller and Data Processor. Darktrace is committed to complying with data protection legislation and good practice. Darktrace has a designated Data Protection Officer contactable at privacy@darktrace.com.

23. Dispensations

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