Introduction

Ashtead Technology recognises the significance of Sanctions and AML Laws that have been imposed and enacted by the jurisdictions in which Ashtead Technology conducts business and/or to which Ashtead Technology has a relevant nexus.

Ashtead Technology is committed to full compliance with all applicable Sanctions and AML Laws, as well as to applicable guidelines and standards that comprise best business practices. The purpose of this Sanctions, Anti-Money Laundering and Counter Terrorist Financing Policy (the "Policy") is to support and enable compliance by Ashtead Technology and each Employee with AML laws and Sanctions, to assist law enforcement in combating money laundering, terrorism financing, and other illegal activities, and to minimise the risk of Ashtead Technology being used for improper purposes.

To this end, Ashtead Technology has adopted a group-wide compliance program comprised of risk-based policies, procedures and internal controls (the "Compliance Program") designed to detect and prevent the use of Ashtead Technology to facilitate money laundering, terrorist financing, and other illegal activities, which are set forth in this Policy.

Failure to comply with Sanctions and AML Laws could result in civil and/or criminal penalties to Ashtead Technology and/or individual Employees. As such, it is imperative that every Employee is familiar with and complies with the provisions set forth in this Policy in order to protect Ashtead Technology from being used to facilitate money laundering, terrorist financing and other crimes. The provisions of this Policy will be strictly enforced.

Scope

This policy applies to all Employees. Ashtead Technology will ensure that these persons are made aware of the law and the requirements of this policy.

Any Employee who violates this Policy may be subject to disciplinary action.

This policy applies to the Ashtead Technology group globally. Individual Ashtead Technology Group companies may have additional local policies and procedures designed to comply with their local legislation, regulations and any government approved guidance in the jurisdiction(s) in which they operate. Notwithstanding this Policy, Employees are required to adhere to all applicable legislation, regulations and government approved guidance in the jurisdiction(s) in which they operate

Definitions

Word	Definition
AML	Anti-Money Laundering
AML Laws	Applicable money laundering statues of all jurisdictions, including laws aimed at countering the financing of terrorism, the rules and regulations thereunder and any related or similar rules, regulations or guidelines, issued, administered or enforced by any governmental agency, including but not limited to POCA and the TA.
Ashtead Technology	All entities within the Ashtead Technology group of companies being; Ashtead Technology Holdings plc, BP INV2 Pledgeco Ltd, Ashtead Technology Ltd, Alfred Cheyne Engineering Ltd, Ashtead Technology (SEA) Pte Ltd, Ashtead Technology LLC, Ashtead Technology (Canada) Ltd, Ashtead Technology AS, Seascan Ltd, Seatronics Ltd, Ashtead US Pledgeco Inc, Ashtead Technology Offshore Inc, Ace Winches Inc and Seatronics Inc, and any other subsidiaries of Ashtead Technology Holdings plc from time to time.
Board	The Board of Ashtead Technology Holdings plc
Compliance Officer	This may be an employee nominated within a firm to undertake suspicious activity reporting and liaise with the NCA where required. In the Compliance Officer's capacity as the Money Laundering Reporting Officer, they maintain ultimate responsibility for the anti-money laundering controls and affairs of the firm. In the Compliance Officer's capacity as the Nominated Officer they can be personally criminal liable for failing to report knowledge or suspicion of money laundering under section 332 POCA.
CTF	Counter-terrorist financing
Director	A member of the Board of directors of any Ashtead Technology entity
Employee	All individuals working at all levels, bands and grades within Ashtead Technology, including Directors, senior management, officers,

	employees (whether permanent, fixed term, part-time or temporary); as well as contractors, seconded staff, consultants, agents, interns, sponsors and any other person associated with Ashtead Technology, or its subsidiaries or their employees, wherever located.
FATF	The Financial Action Task Force which lays down international AML and CTF standards
NCA	The National Crime Agency is an Executive Non-Departmental Public Body (NDPB) of the Home Office. NCA officers can have the combined powers of police, customs and immigration officers and also have a substantial range of tools and legislation to target criminals with.
HMRC	His Majesty's Revenue and Customs
POCA	Proceeds of Crime Act 2002
OFAC	The Office of Foreign Assets Control of the US Department of the Treasury
Risk Committee	The Ashtead Technology internal Risk Committee
Sanctions	Economic or financial sanctions or trade embargoes imposed, administered or enforced from time to time by (i) the United Nations, (ii) the United States, (iii) the European Union, (iv) any member state of the European Union, (v) the United Kingdom, (vi) any other applicable jurisdiction, or (vi) the respective governmental institutions of any of the foregoing including, without limitation, OFAC, the US Department of Commerce, the US Department of State and any other agency of the US government, or Her Majesty's Treasury of the United Kingdom
SAR	A formal suspicious activity report to be submitted by the Compliance Officer to the NCA or country equivalent
TA	Terrorism Act 2000

Legal framework for AML and sanctions

Various jurisdictions have enacted AML Laws directed at preventing the use of the financial system for money laundering, terrorist financing, and other financial crimes and have imposed sanctions programs that restrict the conduct of governments, entities or individuals of certain countries. The AML Laws generally exist to prevent persons involved in criminal activity—such as terrorism, drug trafficking or corruption—from committing acts to conceal or disguise the criminal origins of their money. Sanctions programs generally seek to pressure Sanctions targets into modifying their behaviour or otherwise isolate those targets from the global economic system.

AML Laws

Money laundering is generally defined as the practice of concealing or disguising the origins of proceeds derived from criminal activity, such as drug trafficking, fraud, bribery or organised crime, by creating the appearance that the proceeds are derived from a legitimate source. Terrorist financing is the provision of funds or "material support" for terrorist activities through illegal activity, such as drug trafficking, counterfeiting, and credit card fraud.

Overview of legislative and regulatory framework in the UK

POCA and the TA are the key AML Laws in the UK. The key money laundering offences in POCA relate to handling criminal property (e.g. by acquiring, using, possessing, concealing or transferring it), or being involved in an arrangement that facilitates the handling of criminal property by a third party. In addition, if a Compliance Officer knows or suspects that someone is engaged in money laundering (further to an internal report) and fails to report it to the NCA as soon as practicable, the Compliance Officer commits an offence. It is also an offence to prejudice a money laundering investigation (e.g. by alerting the person suspected of money laundering that a report has been made to the NCA, or by destroying relevant documents).

The key CTF offences in the TA relate to raising, possessing or handling funds or other property or a terrorist purpose (whether or not those funds are from criminal activity), being involved in arrangements to fund terrorist, and laundering terrorist property.

Knowledge or suspicion of money laundering or terrorist financing offence

Employees are required to record and promptly report to the Compliance Officer any knowledge or suspicion that another person has committed a money laundering offence or a terrorist financing offence in order for an assessment to be made by the Compliance Officer. The assessment undertaken by the Compliance Officer will determine whether a SAR should be submitted to the NCA or country equivalent.

An Employee may think that a transaction is suspicious without needing to know the exact nature of the criminal offence or that particular funds definitely arose from a crime. An Employee may have noticed something unusual or unexpected and after making enquiries, the facts do not seem normal or do not make commercial sense. An Employee does not have to have evidence that money laundering is taking place to have suspicion.

After making a report, Employees (save for the Compliance Officer) should take no further action (such as entering into a transaction or paying a questionable invoice etc.), in order to avoid committing the criminal offence of "prejudicing an investigation" or any other offence.

Sanctions Programmes

Economic or financial sanctions are measures imposed by national governments and multinational bodies which seek to alter the behaviour and decisions of other national governments or non-state actors that may (i) threaten the security of the global community, or (ii) violate international norms of behaviour (e.g. human rights violations), amongst other things.

Sanctions applicable to Ashtead Technology include economic or financial sanctions or trade embargoes imposed, administered or enforced from time to time by (i) the United Nations, (ii) the United States, (iii) the European Union, (iv) any member state of the European Union, and (v) the United Kingdom.

EU, UK and US Sanctions regimes

The EU imposes an asset freeze on designated persons, entities, and bodies (along with other sanctions measures targeting certain third countries). The EU External Action Service maintains a global list of parties subject to an asset freeze where all designated parties are listed. Certain competent EU Member State government agencies may also maintain their own asset freeze lists (including the EU designated parties). The EU and its Member States also impose general export controls on military and dual-use items, including when such items are brokered by EU parties in third countries.

The UK has its own sanctions regime, which is currently similar to the EU's regime.

HM Treasury's Office for Financial Sanctions Implementation ("OFSI") provides a consolidated list of persons and organisations subject to UK financial sanctions.

In the US, the Office of Foreign Assets Control of the US Treasury Department ("OFAC") administers and enforces US-based economic and trade sanctions and publishes lists of individuals, groups and entities, such as terrorists and narcotics traffickers, which are subject to US sanctions. These include: the Specially Designated Nationals ("SDNs") and Blocked Persons List ("SDN List"), the Foreign Sanctions Evaders List ("FSE List"), and the Sectoral Sanctions Identifications List ("SSI List") (collectively, "OFAC Lists"). The US also maintains "secondary sanctions" programs that allow the US to impose sanctions on any non-US entity that engages in targeted activities, even if those activities do not violate US law or the laws of the non-US person's home jurisdiction.

Ashtead Technology generally applies US sanctions regimes as if it is a US person. This is done for a number of reasons, including management of business and reputational risk, and because US sanctions regimes apply to persons located in the US and in many cases to non-US companies, such as, for example, if a transaction that takes place outside the United States between non-US persons calls for payment in US dollars.

Responsibility for compliance with this policy

The responsibility of ensuring compliance with Ashtead Technology's policy and ensuring effective controls to prevent money laundering and terrorist activity vests with all Employees. Notwithstanding, there is a varying level of responsibility across the organisation to deter money laundering and terrorist activity depending on the performance of a certain role or function within the organisation. Below is a non-exhaustive list of responsibilities within the organisation that vest within a role or function.

If despite having received training and completed the relevant competency requirements within the organisation, there is any doubt in relation to the responsibilities under this policy and the guidance issued from time to time, the relevant Employee or function must consult the Compliance Officer.

Board responsibility

To monitor and assess the adequacy and effectiveness of Ashtead Technology's anti-money laundering systems and controls and review regular reports from executive management.

Risk Committee responsibility

To assess anti-money laundering and counter terrorist risk and ensure actions are taken to address any changes to risk levels.

Senior Management responsibility

To establish effective policies and guidance and be responsible for monitoring their effectiveness.

To ensure Employees are adequately trained in relation to their obligations under this policy and ensuring that employees show an understanding and competence of the AML Laws and their duties to deter and prevent money laundering and terrorist activity.

To ensure a Compliance Officer remains appointed who acts as the person within Ashtead Technology who is responsible for receiving and considering reports from Employees who have money laundering and/or terrorism financing suspicions, and for determining whether a SAR needs to be made to the NCA.

Compliance Officer Responsibility

To be the key point of contact for Employees, police and government investigations and to ensure that any requests to Ashtead Technology for the release of data for the prevention or detection of crime are managed effectively.

- To be the person responsible for receiving, analysing and understanding suspicious activity reports from within the business.
- To undertake initial investigations of reported suspicions.
- To either (i) authorise transactions that have been reported to him or her or (ii) refuse and escalate to the authorities.
- If appropriate, to formally raise a SAR to the NCA (or equivalents in other jurisdictions where applicable).
- To monitor compliance with the policy, regularly reporting to senior management. Senior management will report compliance updates to the Board on a regular basis (and at a minimum quarterly).
- Maintenance and review of this policy.
- Monitor new legislation on money laundering.
- Conducting sanctions screening.
- Advise on technical requirements to ensure compliance with laws, regulations, and guidance in connection with the prevention of money laundering and terrorist activity.

Accounts team responsibility

- To monitor any payments, which are received directly into the accounts department, keeping senior management and the Compliance Officer informed as appropriate.

Customer facing roles and other skilled and technical role (ST) responsibility

- To read, understand and follow the requirements of this policy ensuring any reportable events, and any other suspicions of money laundering/terrorist financing are immediately referred to the Compliance Officer.

- To attend training activities relevant to the requirements of this policy and procedures.

Team leaders and managers responsibility

- To ensure their team members are aware of their responsibilities and follow this policy and procedures
- To ensure they maintain effective governance and controls of this policy.

AML and Sanctions Compliance Programme

To promote compliance with all applicable AML and sanctions laws, Ashtead Technology has adopted and will enforce this AML and Sanctions Compliance Program which sets forth risk-based written policies, procedures and internal controls that are reasonably designed to prevent Ashtead Technology from being used to facilitate money laundering or other illegal activities and cause Ashtead Technology to comply with applicable AML and sanctions laws. The provisions of the AML and Sanctions Compliance Program are discussed in the sections below.

Risk Assessment

The Risk Committee will assess and monitor any movement in risk in relation to anti-money laundering and counter terrorist financing in relation to Ashtead Technology. This will include, amongst other things, whether there have been any changes to the nature of the risks which Ashtead Technology faces and whether there should be any changes made to this policy and the procedures set out herein.

Independent audit

On a periodic basis, but not less than biennially, an independent audit will be conducted of Ashtead Technology's sanctions and AML compliance to monitor and maintain the ongoing effectiveness of the AML Compliance Program and Ashtead Technologies' compliance with the applicable sanctions programs and AML laws. The audit will be conducted by: (i) a qualified third party, such as external auditors; or (ii) an Employee or group of Employee(s) who are knowledgeable regarding applicable sanctions and AML requirements but are not involved in the operation or oversight of the AML/Sanctions Compliance Program, this may include the internal audit function.

The audit will assess, among other things, compliance with applicable AML, Sanctions and this policy, the adequacy of Ashtead Technology's AML and sanctions risk assessment, and the adequacy and effectiveness of Ashtead Technology's AML and sanctions policies and procedures and include testing of all affected areas to ensure that Employees are complying with these policies and procedures. The results of the audit will be submitted to the Compliance Officer, other senior management, and the Board, as appropriate.

Training and compliance

One of the most important controls over the prevention and detection of money laundering and terrorist financing is to have employees who are alert to the risks and are trained in identifying potential suspicious transactions.

All Employees are responsible for reading and having access to the Policy. All Employees will receive compulsory Policy training upon joining Ashtead Technology and regular refresher training. In addition, assigned employees in charge of the customer due diligence and sanctions screening processes will receive training on those processes and

the use of tools necessary in performing their duties. Dates and names of those in attendance at the training will be recorded, with training materials and records kept for the mandatory retention period as required.

The training will cover information that Employees with pertinent job functions should be aware of in regard to their handling or supervision of the handling of customers, transactions and/or funds that may involve suspicious activity. The training will also cover, at a minimum, the following:

- Employees' responsibilities under applicable sanctions programs and AML Laws and terrorist financing laws, as well as their responsibilities under this Policy, including the responsibility for conducting sufficient customer due diligence and for identifying and escalating suspicious activity to the Compliance Officer;
- Red flags and signs of money laundering, terrorist financing and other financial crimes that may arise during the course of the Employee's duties;
- The identity and responsibilities of the Compliance Officer;
- The potential consequences for Employees for non-compliance with applicable sanctions programs and AML Laws, including disciplinary action, as well as civil and criminal penalties; and
- Ashtead Technology's record retention policy in relation to the Policy.

Ashtead Technology, in conjunction with the Compliance Officer, will review its businesses to see if certain Employees, depending on the business in which they are involved, may need to receive further or more specific training, which will be recorded and retained in the same manner as the Ashtead Technology-wide Policy training.

In the event of any revisions in legislation and/or regulatory requirements, this Policy will be updated and Employees will be given additional training to the extent required.

Monitoring, detection and reporting of suspicious activity

US and UK AML Laws generally provide for the monitoring, detection, and in appropriate circumstances, the reporting of suspicious transactions to the relevant authorities. Accordingly, Ashtead Technology has implemented appropriate and risk-based procedures that provide for the identification and scrutiny of transactions that may be related to money laundering, such as, for example, unusual patterns of transactions, transactions that do not match the customer's profile, transactions involving suspicious countries, or transactions that have no apparent economic or lawful purpose.

In the event that an Employee becomes aware of facts and circumstances that may indicate potential money laundering, terrorist financing or other illicit activities, these matters must be promptly reported to the Compliance Officer. Employees should immediately report any "red flags" relating to possible violations to the Compliance Officer, who will determine what actions should be taken by Ashtead Technology, including whether such activity should be reported to the authorities.

Such red flags include, but are not limited to, the following:

- Notification by computerised screening of a customer in relation to countries, persons or entities that are the target of applicable sanctions administered and enforced by the US Government or any other competent government agency;
- Notification by computerised screening of a customer in countries either identified as being non-cooperative with international efforts against money laundering (e.g., by or against whom the US Treasury Department has issued an advisory), or otherwise deemed to be higher risk;
- Refusal or reluctance to disclose or provide documentation concerning identity, nature of business, nature and source of assets;
- Providing false, misleading or substantially incorrect information;
- Refusal or reluctance to identify a principal or beneficial owner of a customer (e.g., a shell company or agent, acting on behalf of an undisclosed third party);

- Engaging in transactions that appear to have been structured so as to avoid government reporting requirements;
- Concern about compliance with government reporting requirements;
- Lack of concern regarding risks or other transaction costs;
- The customer or service provider wishes to engage in a transaction that lacks business sense, economic substance or apparent investment strategy;
- Assets well beyond the customer's or party's known income or resources;
- Request that funds be transferred to a third party, such as an unrelated party or to a jurisdiction other than the one in which the party is located, particularly if located in an 'offshore' bank secrecy or tax haven;
- The customer or party, or any person associated with the customer or party, is or has been the subject of any known formal or informal allegations (including in the reputable media) regarding possible criminal, civil or regulatory violations or infractions;
- The number of employees is unusually low taking into account the scope of the business;
- The customer or party is acquiring assets (e.g. Ashtead Technology products) which do not relate to its business;
- Constituent documents of the customer or party do not reflect the activities performed, although legally required;
- The customer or party makes payments which are disproportionate to its financial capacity;
- The party's invoices show gaps or missing information (e.g., missing VAT-number, account number, invoice number, or address or date);
- Funds are received from, or the customer or party requests that funds are distributed to bank accounts in countries other than the customer's country of origin or residence; or
- Funds are received from, or the customer or party requests that funds are distributed to, bank accounts in countries where drug trafficking or money laundering is known to occur or to other high-risk countries or financial secrecy havens.

All Employees must report promptly to the Compliance Officer when they become aware of facts and circumstances that may indicate potential money laundering, terrorist financing or other illegal activity. The Compliance Officer will consider the circumstances, including whether a report should be made to the relevant authorities, and decide on the appropriate next steps.

Upon further review of a suspicious transaction, if the Compliance Officer determines that the transaction is designed to involve use of Ashtead Technology to facilitate money laundering, terrorist financing, or another illegal activity, Ashtead Technology will refuse to consummate, will withdraw from, or will terminate such transaction, as appropriate.

An Employee who makes a report will not be subject to any retaliation for any reports made in good faith. Employees must not disclose such reports, or information pertaining to a violation of Sanctions or AML Laws which has been included in such reports, to any other person (including the person who is the subject of the report), except as may be required by law or regulation or in connection with an internal review by Ashtead Technology. The Compliance Officer, after consultation with external counsel, will advise the Employee if such an exception applies.

Prohibited relationships with third parties

Ashtead Technology and its Employees may not establish relationships, engage in any transactions or otherwise conduct business with certain customers, vendors, suppliers or other third parties ("Prohibited Third Parties"), including:

- any customer, vendor, supplier or third party whose name appears on the SDN List, or any of the other OFAC Lists, or on OFSI's consolidated list, or on a list from any other relevant agency administering an applicable sanctions program;

- any customer, vendor, supplier or third party owned (by 50% or more) or controlled by a party designated on any of the abovementioned sanctions related lists;
- any customer, vendor, supplier or third party whose name appears on any list of known or suspected terrorists or terrorist organisations issued by the relevant authorities;
- any customer, vendor, supplier or third party whose transaction is known or suspected to constitute or relate to money laundering or terrorist financing; and
- such other lists of prohibited persons and entities as may be mandated by applicable law or regulation.

Politically exposed persons

On occasions, Ashtead Technology may identify someone who has been entrusted with a prominent public function, or an individual who is closely related to or associated with such a person (a "PEP"), who is – or is linked to – a customer or other third party with which Ashtead Technology does business. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. Upon identification of a PEP, enhanced due diligence is required in order to validate the source of any monies to be received by Ashtead Technology, or the destination of any monies to be given by Ashtead Technology. The Compliance Officer will determine what enhanced due diligence is required in these circumstances.

High risk countries

Generally, criminals tend to seek out countries or sectors in which there is a low risk of detection due to weak or ineffective anti-money laundering controls and then move funds through stable financial systems.

Where transactions originate from a high-risk country, enhanced due diligence and/or approval from the senior management and/or Compliance Officer may be required depending on the level of risk posed by the transaction. The Compliance Officer will determine what enhanced due diligence and whether approval is required in these circumstances.

Ashtead Technology has identified a list of Sensitive countries which are categorised from Group 1 – No trade permitted to Group 5 – Countries at higher risk of circumvention. The current list can be found in Appendix III of the Internal Compliance Program.

Reportable Events

Where there is a suspicion, this must be reported to the Compliance Officer by email. Alternatively, you can contact the CEO, CFO, Chairman of the Board or External Auditors, anonymously or otherwise if you do not feel comfortable making the notification via email. The notification should contain all the relevant information that forms the basis of your suspicion to enable a Compliance Officer to make an informed decision on the suspicion.

Once reviewed by the Compliance Officer and investigated, the Employee may be instructed to:

- Obtain further information to assist the Compliance Officer's decision making;
- Accept the payment, where it hasn't already been accepted, as it has been approved as acceptable by the Compliance Officer;
- Not accept or refuse any payment as NCA consent is pending; and/or
- Refuse the offer of payment (whether on the Compliance Officer's recommendation or the NCA's response).

Those who may be involved in the potentially suspicious activity should not be made aware that a report has been made or that a SAR is being considered or filed by the Compliance Officer. Any such disclosure could result in an offence being committed. The Employee should not inform others of their suspicion or the report made without prior approval from the Compliance Officer.

Reports made internally to the Compliance Officer should be made as soon as practicable after the Employee knows

or suspects money laundering, and generally within 24 hours. The Compliance Officer will consider all the circumstances and, if they also know or suspect money laundering, will make a SAR to the NCA.

Consequences of non-compliance

Employees have a strict duty to comply with this Policy and the AML Laws and Sanctions referred to in this Policy.

The Compliance Officer will investigate all reported possible Policy violations promptly and with the highest degree of confidentiality possible under the circumstances. No Employee may conduct any preliminary investigation, unless authorised to do so by the Compliance Officer. Cooperation by Employees in the investigation will be expected. As needed, the Compliance Officer will consult with the legal team or the Directors.

It is Ashtead Technology's policy to employ a fair process by which to determine violations of the Policy. If any investigation indicates that a violation of the Policy has probably occurred, Ashtead Technology will take such action as it believes appropriate under the circumstances.

Failure to comply with this Policy may constitute a disciplinary offence and/or a criminal offence.

Keeping Records

Ashtead Technology will keep full and accurate records in order to monitor and manage our money laundering risks in the business. This will also enable the Compliance Officer to make an adequate report to the NCA. Ashtead Technology therefore has systems and controls in place to keep records of the customer and the transaction(s) involved to the extent permitted by applicable law, for 7 years after the business relationship has ended.

Allan Pirie

Chief Executive Officer

Ashtead Technology Holdings plc and all of its trading subsidiaries including Ashtead Technology Ltd, Ashtead Technology Offshore Inc, Ashtead Technology (South East Asia) Pte Ltd, Ashtead Technology LLC, Ashtead Technology AS, Ashtead Technology (Canada) Ltd and Alfred Cheyne Engineering Ltd

Revision Control

Document Title		**Ashtead Technology Policy Template**	
Revision	Date	Author	**Comments**
2	30/10/25	P McDonald	Template updated to include new footer. Minor amendments/updates
Approver		Allan Pirie	
Author		Philippa McDonald – Compliance Manager	