SYNATRIX

Information Security Standards Policies

Synatrix Ltd policies, standards and working practices

OBJECTIVE

Document Scope

To detail the security policies and working practice requirements regarding the use of all Synatrix Ltd information, IT equipment, services and facilities.

Application of the policies

This policy applies to all Synatrix Ltd employees, contractors and agents (hereafter referred to as 'individuals'). This policy applies to all information, in whatever form, relating to Synatrix Ltd business activities worldwide, and to all information handled by Synatrix Ltd relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Synatrix Ltd or on its behalf.

Monitoring and reviewing

These policies are monitored and reviewed on a regular basis. They will be assessed for suitability, adequacy and effectiveness and will be review at least annually. Synatrix Ltd reserve the right to amend any part of these policies at any time to legitimately improve their effectiveness. Where the need for improvement arises; actions will be carried out promptly to update and apply the policies and procedures contained herein.

Version:	14.2
Approved By:	David Mash
Position:	Company Director – Synatrix Ltd
Approval Date:	2018-10-09
Effective Date:	2018-10-09
Review Period:	Annual

CONTENTS

1 Acceptable use policy 3

1.1 Computer access control and authentication 3

1.2 Password complexity requirements 3

1.3 Internet Access, Email and Messaging Conditions of Use 4

1.4 Telephony (Voice) and Video Conferencing 5

1.5 Monitoring and Filtering 5

1.6 Clear Desk and Clear Screen 5

2 Data Privacy Policy 6

2.1 Scope 6

2.2 Data Processor (outside of Scope) 6

2.3 Data Controller 7

2.4 Information Collected 7

2.5 Protection of the information collected 7

2.6 Access to the Information collected 8

2.7 Retention and Destruction of the information collected 8

2.8 Owner rights of the information collected 9

3 Remote Working Policy 11

3.1 Working off-site 11

3.2 Remote working 11

3.3 Wireless Access and Mobile data 11

4 Software Usage Policy 12

4.1 Software installation and online subscription services 12

4.2 Mobile storage devices 12

4.3 Anti-Virus software 12

4.4 Acceptable Encryption 13

5 Anti-Corruption Policy 14

5.1 Policy statement 14

5.2 Scope 14

5.3 Definition of bribery 15

5.4 What is and what is NOT acceptable 15

6 Information Security Incident Management Policy 17

6.1 Definition of an information security incident 17

6.2 Responsibility to report and react 18

7 Further information 19

7.1 Version control 19

7.2 Help and advice 19

1 ACCEPTABLE USE POLICY

1.1 COMPUTER ACCESS CONTROL AND AUTHENTICATION

Access to the Synatrix Ltd IT systems is controlled using User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Synatrix Ltd IT systems. Use of Synatrix Ltd owned (or rented) equipment and services, operated locally or remotely, must be conducted in accordance with all policies within this document.

Individuals must:

1. Make use of Synatrix Ltd approved multi-factor or biometric authentication where possible.
2. Where a password is used, ensure that the password complexity requirements are observed.
3. Ensure pin-codes consist of at least four numbers and are not the sole means of authentication.
4. Keep passwords safe and secure and ideally make use of a password storage management system that is fully approved and verified by Synatrix Ltd.
5. Ensure that all passwords are unique and, where possible, are associated with a meaningful Synatrix Ltd username or email address that identifies an individual.

Individuals must not:

1. Allow anyone else to use their user ID/token and password on any Synatrix Ltd IT system.
2. Leave their user accounts logged in at an unattended and unlocked computer.
3. Use someone else's user ID and password to access Synatrix Ltd IT systems.
4. Leave their password unprotected (for example writing it down).
5. Perform any unauthorised changes to Synatrix Ltd IT systems or information.
6. Attempt to access data that they are not authorised to use or access.
7. Exceed the limits of their authorisation or specific business need to interrogate the system/data.
8. Connect any non-Synatrix Ltd authorised device to the Synatrix Ltd network.
9. Store Synatrix Ltd data on any non-authorised Synatrix Ltd equipment.
10. Give or transfer Synatrix Ltd data or software to any person or organisation outside Synatrix Ltd without the authority of Synatrix Ltd.

1.2 PASSWORD COMPLEXITY REQUIREMENTS

1. Passwords must be of at least 8 characters in length.
2. Contain characters from each of the following categories:
    - English upper-case letters (A through Z)
    - English lower-case letters (a through z)
    - Numerical digits (0 through 9)
    - Non-alphabetic characters (for example, an exclamation mark or ampersand)

1.3 INTERNET ACCESS, EMAIL AND MESSAGING CONDITIONS OF USE

In this section, the term '**digital communications'** is used to define the following terms:

- Internet – *Any activity,* service *or interaction on the public or private world wide web.*
- Email – *Any email service accessed through an application or online internet browser.*
- Messaging – *Any system that is used to message (instantly or otherwise) any other individual or group by online means via the public or private world-wide-web (www).*

Use of Synatrix Ltd digital communications are intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Synatrix Ltd in any way, not in breach of any term and condition of employment and does not place the individual or Synatrix Ltd in breach of statutory or other legal obligations. All individuals are personally accountable for their actions on digital communications systems.

Individuals must not:

1. Use digital communications for the purposes of harassment or abuse.
2. Use profanity, obscenities, or derogatory remarks in communications.
3. Access, download, send or receive any data (including images), which Synatrix Ltd considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
4. Use digital communications to make personal gains or conduct a personal business.
5. Use digital communications to gamble.
6. Use digital communications in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
7. Place any information on the Internet that relates to Synatrix Ltd, alter any information about it, or express any opinion about Synatrix Ltd, unless they are specifically authorised to do this.
8. Send unprotected sensitive or confidential information externally.
9. Forward Synatrix Ltd mail to personal non-Synatrix Ltd email accounts (for example a personal Hotmail account) unless authorised to do so (for example, testing delivery).
10. Make official commitments through the internet or email on behalf of Synatrix Ltd unless authorised to do so.
11. Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
12. In any way infringe any copyright, database rights, trademarks or other intellectual property.
13. Download or install any software from the internet without prior approval of Synatrix Ltd.
14. Connect Synatrix Ltd devices to the internet using connections that are not expressly installed and approved Synatrix Ltd.

1.4 TELEPHONY (VOICE) AND VIDEO CONFERENCING

Use of Synatrix Ltd voice and conferencing equipment is intended for business use. Individuals must not use these facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

1. Use Synatrix Ltd voice or conferencing facilities for conducting private business.
2. Make hoax or threatening calls (voice or video) to internal or external destinations.
3. Accept reverse charge calls unless it is for authorised business use.
4. Record calls (voice or video) without the approval of Synatrix Ltd and the express consent of all parties on the respective call.

1.5 MONITORING AND FILTERING

All data that is created and stored on Synatrix Ltd equipment is the property of Synatrix Ltd and there is no official provision for individual data privacy. Wherever possible, Synatrix Ltd will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Synatrix Ltd has the right (under certain conditions) to monitor digital communications and call (video or voice) activity on its systems to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

1. Computer Misuse Act 1990 – https://www.legislation.gov.uk/ukpga/1990/18/contents
2. Data Protection Act 2018 – https://www.legislation.gov.uk/ukpga/2018/12/contents

1.6 CLEAR DESK AND CLEAR SCREEN

To reduce the risk of unauthorised access or loss of information, Synatrix Ltd enforces a clear desk and screen policy as follows:

1. Personal or confidential business information must be protected using security features provided, for example secure print on printers.
2. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
3. Care must be taken to not leave confidential material on printers or photocopiers.
4. All business-related printed matter must be disposed of using confidential waste bins or shredders.

2 DATA PRIVACY POLICY

2.1 SCOPE

The scope of this data privacy policy is limited to the data collected for the express processing, collection and transmission of personal data as it pertains directly to the operational business of Synatrix Ltd. It covers how this information is collected, how it is stored and the information owner's rights in relation to it. Synatrix Ltd will comply with the General Data Protection Regulation (GDPR) when dealing with personal data.

For the purposes of the GDPR, Synatrix Ltd will be the "data controller" of the 'information collected' in section 2.4of this policy. Further details on the GDPR can be found at the website for the Information Commissioner (www.ico.gov.uk).

2.2 DATA PROCESSOR (OUTSIDE OF SCOPE)

2.2.1 CLIENT SOLUTIONS

It is important to note that the core business of Synatrix Ltd is to supply and maintain solutions for clients (hereafter referred to as 'client solutions'). Client Solutions may require the collection, processing and transmission of personal data. It is critical to note that the personal data within such solutions is always owned by the client as they are the data-controller of such information. It is the responsibility of the client to fulfil their legal obligation in this regard; ensuring that they have a data privacy policy in place to comply with GDPR.

NB: Synatrix Ltd will always ensure that their clients have full visibility on any personal data collected in client solutions supplied by Synatrix Ltd. This will fully empower the respective client to create a data privacy policy that is fully accurate and transparent for its users.

2.2.2 DATA PROCESSORS AGREEMENTS

To attain full GDPR compliance for the client solution; it is the responsibility of the client to ensure that any suppliers (sub-processors) of their personal data comply with their own data privacy policy. This is achieved by the client forming a legally binding contract with sub-processors to ensure that they meet the minimum-security requirements and policies laid out in their data privacy policy. This is known as a Data-Processor Agreement (DPA). Synatrix Ltd are always open to signing client DPA's and making any adjustments required to support GDPR compliance.

In the preceding section, it is noted that Synatrix Ltd may be requested by its clients to be a 'data-processor' for the client's (the data-controller) data. As such, it is the responsibility of each Synatrix Ltd client to ensure that they have a data privacy policy that fully covers the information collected by their solution. Synatrix Ltd will work with clients to ensure that they are able to fulfil their obligations as a data-controller (under GDPR). This will include, but is not limited to, ensuring that the client can form a suitable written contract to cover data-processing that may not be covered in other standard contracts or agreements.

2.3 DATA CONTROLLER

Synatrix Ltd is a company with UK registration number: 10662012. The companies registered address is shown below along with the main contact email telephone number:

Company Address:

Synatrix Ltd
156 Broad Hinton, Twyford,
Reading, Berkshire, England,
RG10 0XH

Contact Information:

Email: dpo@synatrix.co.uk
Telephone: +44 (0)7818 003 672

Company Registration: 10662012

2.4 INFORMATION COLLECTED

Information collected	Purposes	Legal basis of processing
A prospect's contact details: person's name, company-name, company-email and direct company telephone number(s).	A prospect has proactively contacted Synatrix Ltd and chosen to share such information in-line with this agreement.	Responding to the prospects request in their legitimate interest in forming a future contract with Synatrix Ltd
The client's company-name, registration number, registered address and main company telephone/fax numbers.	To manage the clients credit limit and to allow client invoicing.	Performing the contract between Synatrix Ltd and the client.
The client's main contact details: person's name, company-email and direct company telephone number(s).	To keep the client up-to-date with their projects.	

NB: The information collected in the table above will hereafter be referred to as "information collected".

2.5 PROTECTION OF THE INFORMATION COLLECTED

1. To perform the contract with the client, it may sometimes be necessary for Synatrix Ltd to transfer the information collected outside of the European Union. Where this occurs, Synatrix Ltd will only do so in accordance with the GDPR. This is most likely to involve either;
    - Approval by the EU Commission that the country to which the information collected is being transferred provides adequate protection for personal data
    - A standard clause basis, required by the EU, with the organisation to which Synatrix Ltd are transferring the information collected.

2. Synatrix Ltd have implemented generally accepted standards of technology and operational security to protect the information collected from loss, misuse, or unauthorised alteration or destruction. These security standards are detailed throughout this policy document.
3. It should be noted that where the client communicates any element of the information collected to Synatrix Ltd; the transmission and security from the client to Synatrix Ltd cannot be guaranteed as 100% secure or in line with Synatrix Ltd security policies.
4. Should any data breach occur; Synatrix Ltd will promptly notify the owner(s) of the information collected in accordance with the Information Security Incident Management Policy (section 6within this document).

2.6 ACCESS TO THE INFORMATION COLLECTED

1. The information collected will never be sold by Synatrix Ltd.
2. Synatrix Ltd will not share the information collected with third parties without the information owners consent except where;
    - there is a legal obligation to do so (for instance company financial filings).
    - It is necessary to fulfil the client's contract and provide agreed services.
3. Where the information collected is disclosed to a third-party; Synatrix Ltd will have a Data Processor Agreement (DPA) in place. This will legally require the third-party to perform their role as a data-processor in accordance with the Synatrix Ltd data privacy policy. This contract will expressly state that the third party must keep the information collected secure and not to use it for their own purposes.
4. It is possible that third parties may themselves engage others (sub-processors) to process the information collected. Third parties will be required to have a DPA in place for each sub-processor where this is the case.

2.7 RETENTION AND DESTRUCTION OF THE INFORMATION COLLECTED

1. Synatrix Ltd will hold the information collected on Synatrix Ltd systems, in accordance with the Synatrix Ltd security policies laid out in this document. This will be for the period that the client is considered an 'active client' or 'active prospect' (defined below).
    - An 'active client' is defined as a company or individual with a presently active product or service supplied by Synatrix Ltd or for a period of 36 months after a project has been completed where;
        i. It is necessary for Synatrix Ltd to comply with its legal obligations.
        ii. it is in the client's legitimate interests to do so (e.g. support and warranties).
    - An 'active prospect' is defined as an individual or company that has chosen to contact Synatrix Ltd and share their information with a view to possibly form a future contract for goods and services provided by Synatrix Ltd. An Active prospect's information will be held for no longer than a period of 12 months from the last point of communication by either party.
2. The information collected will be reviewed annually to establish whether Synatrix Ltd are still entitled to store and process it. If Synatrix Ltd decide that it is not entitled to do so, the information collected will no longer be stored or processed and it will be removed from all services utilised by Synatrix Ltd pursuant to the archival statement below.
3. Removal of the information collected will be carried out in full except where it is strictly required for Synatrix Ltd to comply with legal requirements including, but not limited to;
    - compliance with tax requirements and exemptions.
    - establishment, exercise or defence of legal claims.
4. Synatrix Ltd will ensure that the information collected is securely destroyed once there is no need legitimate need for its' use.

2.8 OWNER RIGHTS OF THE INFORMATION COLLECTED

It is important to that the information owner clearly understand their rights with regards to any of their Personal Data. Where this data is collected by Synatrix Ltd, the owner's rights are detailed below and can be exercised by sending an email to dpo@synatrix.co.uk.

The following rights are attributed to the owner of the information collected (section 2.4 above) hereafter referred to as the 'information owner'.

2.8.1 THE RIGHT TO BE INFORMED

Knowing how Synatrix Ltd will use the information owner's data.

The information owner has the right to be told how Synatrix Ltd will use their Personal Data. This is detailed in section 2.4of this document.

2.8.2 THE RIGHT OF ACCESS

Being provided with copies of the information owner's data.

The information owner has the right to ask Synatrix Ltd to provide them with a copy of their Personal Data. Synatrix Ltd will supply any such information to the information owner as soon as possible but may take up to one month once the requester's identity is verified. Synatrix Ltd will not charge for this process. This is called a data subject access request.

2.8.3 THE RIGHT TO RECTIFICATION

Changing incorrect information held by Synatrix Ltd.

If the information owner believes that the records at Synatrix Ltd are inaccurate; they have the right to ask for the records concerned to be updated.

2.8.4 THE RIGHT TO BE FORGOTTEN

Requesting deletion of the information owner's data.

In some cases, the information owner has the right to be forgotten entirely. This is called data subject information erasure. The information will be removed subject to section 2.7.

2.8.5 THE RIGHT TO RESTRICT PROCESSING

Limiting how Synatrix Ltd may use the information owner's data.

In certain situations, the information owner has the right to ask Synatrix Ltd to restrict the processing of their Personal Data because there is some disagreement about its accuracy or legitimate usage.

2.8.6 THE RIGHT TO DATA PORTABILITY

Moving the information owner's data in a useable format.

The information owner has the right to request the Personal Data provided to Synatrix Ltd in a structured, intelligible and machine-readable format and/or transmit that data to a third party - in certain situations.

2.8.7 THE RIGHT TO OBJECT

When Synatrix Ltd must stop processing the information owner's data.

The information owner has the right to object to Synatrix Ltd processing data purely for the legitimate interests of Synatrix Ltd. When such requests arise, Synatrix Ltd must stop processing the information owner's personal data unless:

- Synatrix Ltd can demonstrate compelling legitimate grounds for the processing, which override the information owner's interests, rights and freedoms.
- The processing is for the establishment, exercise or defence of legal claims.

2.8.8 THE RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

This means Synatrix Ltd making and acting on a decision regarding the information owner based solely by automated means and without any human involvement. The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning the information owner or similarly significantly affects the information owner. Synatrix Ltd does not undertake automated decision making or profiling.

2.8.9 THE RIGHT TO ESCALATE CONCERNS OR COMPLAINTS

The information owner has the right to take any complaints about Synatrix Ltd process their personal data to the Information Commissioner:

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF

Telephone: 0303 123 1113
Website: https://ico.org.uk/concerns/

For further information on each of those rights, including the circumstances in which they apply please see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights under the General Data Protection Regulation.

3 REMOTE WORKING POLICY

3.1 WORKING OFF-SITE

It is accepted that Synatrix Ltd laptops, mobile devices and media will be taken off-site (hereafter referred to as 'offsite equipment'). It is imperative that individuals understand that the following controls must be applied:

1. Offsite equipment must not be left unattended in public places and not left in sight in a car. Laptops must be carried as hand luggage when travelling.
2. Where possible, offsite equipment must be secured in accordance with the authentication and encryption methods detailed within this document.
3. Any loss or compromise offsite equipment must be reported promptly in-line with the Synatrix Ltd incident reporting policy.

3.2 REMOTE WORKING

Remote working is defined as accessing the facilities (services, equipment) of Synatrix Ltd from a remote source (such as home, third-party office or public location). The following considerations must be strictly observed:

1. Only connect to Synatrix Ltd locally hosted facilities by means of an authorised Virtual Private Network (VPN) where possible.
2. Ensure that Synatrix Ltd information is not retained on any unauthorised remote systems in any capacity.
3. Never make connections that require use of intermediary certificates or security services that are not expressly authorised and approved by Synatrix Ltd. This is because, by doing so, the intermediate party could decrypt the encrypted data in transmission.

3.3 WIRELESS ACCESS AND MOBILE DATA

It is understood that wireless networks and mobile-data (for example an individual's phone contract) may be required to access Synatrix Ltd facilities. When doing so, it is critical to observe the following conditions:

1. Wireless networks must only be used if authorised by Synatrix Ltd.
2. Public wireless networks may only be utilised with the express agreement of Synatrix Ltd and can only be used to access Synatrix Ltd facilities if an authorised VPN is used to generate a secure tunnel within the wireless network used.
3. If in any doubt, do not use the wireless network or mobile-data account and, instead, contact an authorised member of Synatrix Ltd to seek guidance and approval.

4 SOFTWARE USAGE POLICY

4.1 SOFTWARE INSTALLATION AND ONLINE SUBSCRIPTION SERVICES

Individuals are only authorised to install and use software or subscription services on Synatrix Ltd owned computer hardware where they are approved and authorised by Synatrix Ltd. Authorised software must be used in accordance with the supplier's licensing agreements. All software or subscription services on Synatrix Ltd hardware must be approved and installed by an approved Synatrix Ltd representative.

Software code of practice:

1. Do not install any software on Synatrix Ltd computer hardware without the approval if an authorised Synatrix Ltd representative.
2. All licensing information for installed software must be retained and securely transmitted to Synatrix Ltd central licensing repository.
3. If you are unsure if the software is authorised to be used; contact an authorised member of the Synatrix Ltd IT team for clarification and guidance.
4. Do not store personal files such as music, video, photographs or games on Synatrix Ltd hardware.

4.2 MOBILE STORAGE DEVICES

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Synatrix Ltd authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Mobile data storage code of practice:

1. Only store information on mobile devices where necessary.
2. Only use authorised Synatrix Ltd devices. Personal devices may be used if they are approved by Synatrix Ltd and the Synatrix Ltd Encryption policy is observed.
3. Mobile devices must be fully accounted for and, in the event of loss or damage, an incident report must be submitted immediately in line with Synatrix Ltd Incident report policy.

4.3 ANTI-VIRUS SOFTWARE

Synatrix Ltd will ensure that anti-virus is installed and implemented on all company owned devices that have the possibility of running anti-virus software. Where possible, the anti-virus software (or service) will be centralised with automated virus detection and virus software updates within the Synatrix Ltd. If a virus is detected and cannot be successfully removed; an incident report must be raised in accordance with the Synatrix Ltd incident report policy.

Individuals must not:

1. Remove or disable anti-virus software.
2. Attempt to remove virus-infected files or clean up an infection, other than using approved Synatrix Ltd anti-virus software and procedures.

4.4 ACCEPTABLE ENCRYPTION

The purpose of this policy is to provide guidance that limits the use of encryption within Synatrix Ltd to only those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that the appropriate regulations are followed by individuals, and that appropriate legal authority is granted for the dissemination and use of each encryption technology.

4.4.1 ALGORITHM REQUIREMENTS

1. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption although other standard can be used with a minimum key length of 256 bits for asymmetric key encryption and 2048 buts for symmetric key encryption.
2. Algorithms in se must meet or exceed published and agreed requirements that reasonably prevent any brute force attempts using industry standard computing power.
3. The common 3DES (or triple DES) algorithm is to be avoided due to its notable compromise.
4. Acceptable Cypher Suite Algorithms

Function	Algorithm
Key Exchange	RSA, Diffie-Hellman, ECDH, SRP, PSK
Authentication	RSA, DSA, ECDSA
Bulk Ciphers	RC4, AES
Message Authentication	HMAC-SHA256, HMAC-SHA1, HMAC-MD5

4.4.2 HASH FUNCTION REQUIREMENTS

In general, adheres to the NIST Policy on Hash Functions:
https://csrc.nist.gov/projects/hash-functions/nist-policy-on-hash-functions

4.4.3 KEY AGREEMENT AND AUTHENTICATION

1. Key exchanges must use one of the following cryptographic protocols defined in the table above.
2. End-points must be authenticated prior to the exchange or derivation of session keys.
3. Public keys used to establish trust must be authenticated prior to use.
4. All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted root provider (or a trusted intermediary certificate).
5. All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider (or a trusted intermediary certificate).
6. Where Synatrix Ltd is responsible for SSL certificates; monitoring from a verified service provider should be implemented to ensure certificates are valid and fully operational.

4.4.4 KEY GENERATION

1. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise and key generation must be seeded from an industry standard random number generator (RNG).

5 ANTI-CORRUPTION POLICY

This anti-bribery policy exists to set out the responsibilities of the individuals working for and with Synatrix Ltd regarding observing and upholding a zero-tolerance position on bribery and corruption. It also exists to act as a source of information and guidance for those individuals to help them recognise and deal with bribery and corruption issues, as well as understand their responsibilities.

5.1 POLICY STATEMENT

Synatrix Ltd is committed to conducting business in an ethical and honest manner and is committed to implementing and enforcing systems that ensure bribery is prevented. Synatrix Ltd has zero-tolerance for bribery and corrupt activities. Synatrix Ltd are committed to acting professionally, fairly, and with integrity in all business dealings and relationships, wherever in the country we operate.

Synatrix Ltd will constantly uphold all laws relating to anti-bribery and corruption in all the jurisdictions in which it operates. Synatrix Ltd are bound by the laws of the UK, including the Bribery Act 2010, regarding the companies conduct both at home and abroad.

Synatrix Ltd recognises that bribery and corruption are punishable by up to ten years of imprisonment and a fine. If Synatrix Ltd is discovered to have taken part in corrupt activities, it is understood that the company may be subjected to an unlimited fine, be excluded from tendering for public contracts, and face serious damage to the company's reputation. Synatrix Ltd commits to preventing bribery and corruption within the business and takes this legal responsibility seriously.

5.2 SCOPE

This anti-bribery policy applies to all employees (whether temporary, fixed-term, or permanent), consultants, contractors, trainees, seconded staff, home workers, casual workers, agency staff, volunteers, interns, agents, sponsors, or any other person or persons associated with u Synatrix Ltd (including third parties), or any of our subsidiaries or their employees, no matter where they are located (within or outside of the UK). The policy also applies to Officers, Trustees, Board, and/or Committee members at any level.

In the context of this policy, third-party refers to any individual or organisation that Synatrix Ltd meets and works with. It refers to actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies – this includes their advisors, representatives and officials, politicians, and public parties.

5.3 DEFINITION OF BRIBERY

1. Bribery refers to the act of offering, giving, promising, asking, agreeing, receiving, accepting, or soliciting something of value or of an advantage so to induce or influence an action or decision.
2. A bribe refers to any inducement, reward, or object/item of value offered to another individual to gain commercial, contractual, regulatory, or personal advantage.
3. Bribery is not limited to the act of offering a bribe. If an individual is on the receiving end of a bribe and they accept it, they are also breaking the law.
4. Bribery is illegal. Employees must not engage in any form of bribery, whether it be directly, passively (as described above), or through a third party (such as an agent or distributor). They must not bribe a foreign public official anywhere in the world. They must not accept bribes in any degree and if they are uncertain about whether something is a bribe or a gift or act of hospitality, they must seek further advice from Synatrix Ltd management.

5.4 WHAT IS AND WHAT IS NOT ACCEPTABLE

5.4.1 GIFTS AND HOSPITALITY

Synatrix Ltd accepts normal and appropriate gestures of hospitality and goodwill (whether given to/received from third parties) so long as the giving or receiving of gifts meets the following requirements:

1. It is not made with the intention of influencing the party to whom it is being given, to obtain or reward the retention of a business or a business advantage, or as an explicit or implicit exchange for favours or benefits.
2. It is not made with the suggestion that a return favour is expected.
3. It follows compliance with local law.
4. It is given in the name of the company, not in an individual's name.
5. It does not include cash or a cash equivalent (e.g. a voucher or gift certificate).
6. It is appropriate for the circumstances (e.g. giving small gifts around Christmas or as a small thank you to a company for helping with a large project upon completion).
7. It is of an appropriate type and value and given at an appropriate time, considering the reason for the gift.
8. It is given/received openly, not secretly.
9. It is not selectively given to a key, influential person, clearly with the intention of directly influencing them.
10. It is not above a certain excessive value of £100.
11. It is not offer to, or accepted from, a government official or representative or politician or political party, without the prior approval of the Synatrix Ltd.

Where it is inappropriate to decline the offer of a gift (i.e. when meeting with an individual of a certain religion/culture who may take offence), the gift may be accepted so long as it is declared to Synatrix Ltd management, who will assess the circumstances.

Synatrix Ltd recognises that the practice of giving and receiving business gifts varies between countries, regions, cultures, and religions, so definitions of what is acceptable and not acceptable will inevitably differ for each.

As good practice, gifts given and received should always be disclosed to Synatrix Ltd management. Gifts from suppliers should always be disclosed. The intention behind a gift being given/received should always be considered. If there is any uncertainty, the advice of Synatrix Ltd management should be sought.

5.4.2 FACILITATION PAYMENTS AND KICKBACKS

Synatrix Ltd does not accept and will not make any form of facilitation payments of any nature. Synatrix Ltd recognise that facilitation payments are a form of bribery that involves expediting or facilitating the performance of a public official for a routine governmental action. Synatrix Ltd recognise that they tend to be made by low level officials with the intention of securing or speeding up the performance of a certain duty or action.

Synatrix Ltd does not allow kickbacks to be made or accepted. We recognise that kickbacks are typically made in exchange for a business favour or advantage. Synatrix Ltd recognises that, despite their strict policy on facilitation payments and kickbacks, employees may face a situation where avoiding a facilitation payment or kickback may put their/their family's personal security at risk. Under these circumstances, the individual must carry out the following steps:

- Keep any amount to the minimum.
- Ask for a receipt, detailing the amount and reason for the payment.
- Create a record concerning the payment.
- Report this incident to Synatrix Ltd management.

5.4.3 5.10 POLITICAL CONTRIBUTIONS

Synatrix Ltd will not make donations, whether in cash, kind, or by any other means, to support any political parties or candidates. We recognise this may be perceived as an attempt to gain an improper business advantage.

5.4.4 5.11 CHARITABLE CONTRIBUTIONS

Synatrix Ltd accepts (and indeed encourages) the act of donating to charities – whether through services, knowledge, time, or direct financial contributions (cash or otherwise) – and agrees to disclose all charitable contributions it makes. Employees must be careful to ensure that charitable contributions are not used to facilitate and conceal acts of bribery. Synatrix Ltd will ensure that all charitable donations made are legal and ethical under local laws and practices, and that donations are not offered/made without the approval of Synatrix Ltd management.

6 INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

This policy is a constituent and critical part of the overall information security standards policy document which sets out a framework of governance and accountability for the management of information security across Synatrix Ltd. Information security is taken extremely seriously by Synatrix Ltd. It is therefore necessary to take prompt action in the event of any actual or suspected breaches of information security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the company.

This policy provides a framework for reporting and managing:

- Information security incidents affecting the Synatrix Ltd information and IT systems
- Incidents affecting any data controlled or processed by Synatrix Ltd
- Loss, disclosure, or corruption of information or devices
- Near misses and information security concerns

6.1 DEFINITION OF AN INFORMATION SECURITY INCIDENT

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of Synatrix Ltd information, in any format, or IT systems in which this information is held. What may appear to be a physical security or IT issue may also be an information security incident and vice-versa.

Examples of an information security incidents can include but are not limited to:

1. Accidental or deliberate disclosure of information to unauthorised individuals e.g. an email containing unencrypted personal information sent to unintended recipients.
2. Unauthorised sharing of information with an external cloud storage service or contractor.
3. Loss or theft of paper or electronic records, or equipment such as tablets, laptops and smartphones or other devices on which data is stored.
4. Inappropriate access controls allowing unauthorised use of information.
5. Suspected breach of Synatrix Ltd IT Acceptable Use Policy.
6. Attempts to gain unauthorised access to computer systems, e.g. hacking.
7. Records altered or deleted without authorisation by the ‘information owner’.
8. Introduction of malware into a computer or network, e.g. a phishing or ransomware attack.
9. Denial-of-service or other cyber-attack on Synatrix Ltd IT systems or networks.
10. A power outage that affects access to Synatrix Ltd IT systems and information services.
11. “Blagging” offence where information is obtained by deception (i.e. social exploits).
12. Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible area.
13. Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information.
14. Audible discussion of confidential topics in public or unauthorised recording of meetings.

6.2 RESPONSIBILITY TO REPORT AND REACT

This policy relies upon timely reports of actual or suspected information security incidents. This is critical to allow such reports to be investigated, resolved and reported upon in a timely fashion to minimise harm and provide the best possible information security.

Individuals must:

1. Minimise the risk of vital or confidential information being lost or falling into the hands of people who do not have the right to see it.
2. Protect the security and integrity of IT systems on which vital or confidential information is held and processed.
3. Report all actual or suspected information security incidents immediately on discovery to dpo@synatrix.co.uk | +44 (0)7818 003 672.

Synatrix Ltd will commit to:

1. Immediately investigate any actual or suspected information security incidents.
2. Work with any third parties and vendors that may be associated with the provision, storage or transmission of data relating to the security incident.
3. Report such incidents, where necessary, to the relevant legal authorities.
4. Liaise with the Information Commissioner's Office and report breaches in line with regulatory requirements to report any data breach that is likely to result in a risk to the rights and freedoms of data subjects within 72 hours of discovery.

7 FURTHER INFORMATION

7.1 VERSION CONTROL

Version #	Approval Date	Approver	Brief description of amendment
V14.2	2018-10-09	David Mash	Updated policy – Grammatical and readability improvements.
v14.1	2018-06-15	David Mash	Refreshed policy based upon latest policies and procedures regarding GDPR. Not yet fully GDPR compliant.
v10.0	2017-12-21	David Mash	Initial version of consolidated documents

7.2 HELP AND ADVICE

The information provided in this document is safe to reside in the public domain and may be distributed but is subject to Synatrix Ltd copyright. Should any clarification be required regarding any element of this document, please contact:

Compliance Manager: David Mash
Company Director – Synatrix Ltd

Email: dpo@synatrix.co.uk
Telephone: +44 (0)7818 003 672

Registered address: 156 Broad Hinton, Twyford, Reading, Berkshire, England, RG10 0XH