INFORMATION SECURITY POLICY STATEMENT

1.0. Policy Objective

1.0. To protect the information assets that Lewis & Graves Partnership Ltd handles, stores, exchanges, processes and has access to, and to ensure the ongoing maintenance of their confidentiality, integrity, and availability.

1.1. To ensure controls are implemented that provide protection for information assets and are proportionate to their value and the threats to which they are exposed.

1.2. To ensure the organisation complies with all relevant legal, customer and other third-party requirements relating to information security.

1.3. To continually improve the organisation's Information Security Management System (ISMS) and its ability to withstand threats that could potentially compromise information security.

2.0. Scope

2.0. This policy and its sub-policies apply to all people, processes, services, technology and assets detailed in the **Scope**. It also applies to all employees or subcontractors of information security critical suppliers who access or process any of the organisation's information assets.

3.0. Core Policy

3.0. The organisation believes that despite the presence of threats to the security of such information, all security incidents are preventable.

3.1. The Directors of Lewis & Graves Partnership Ltd are committed to achieving the objectives detailed in the policy through the following means:

3.1.1. The implementation and maintenance of an ISMS that is independently certified as compliant with ISO 27001:2017;

3.1.2. The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures;

3.1.3. Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures;

3.1.4. The maintenance of a risk treatment plan that is focused on eliminating or reducing security threats;

3.1.5. The maintenance and regular testing of a **Business Continuity Plan**;

3.1.6. The clear definition of responsibilities for implementing the ISMS;

3.1.7. The provision of appropriate information, instruction and training so that all employees are aware of their responsibilities and legal duties, and can support the implementation of the ISMS;

3.1.8. The implementation and maintenance of the sub-policies detailed in this policy.

3.2. The appropriateness and effectiveness of this policy, and the means identified within it, for delivering the organisation's commitments will be regularly reviewed by Top Management.

3.3. The implementation of this policy and the supporting sub-policies and procedures is fundamental to the success of the organisation's business and must be supported by all employees and contractors who have an impact on information security as an integral part of their daily work.

3.4. All information security incidents must be reported to the Compliance Manager. Violations of this policy may be subject to the organisation's **Disciplinary and Appeals Policy and Procedure**.

Signed

James Abbott, Operations Director Reviewed November 2022

Sub-policy index

4.0. Responsibilities

4.0. It is the responsibility of the IT Manager to ensure that this policy is implemented and that any resources required are made available.

4.1. It is the responsibility of the Compliance Manager to monitor the effectiveness of this policy and report the results at management reviews.

4.2. It is the responsibility of the IT Manager to create and maintain an **Asset and Risk Assessment Register** and to ensure all assets that need to be covered by this policy are identified.

4.3. It is the responsibility of all employees and subcontractors, and employees and subcontractors of information security critical suppliers, to adhere to this policy and report to the IT Manager any issues they may be aware of that breach any of its contents.

5.0. Definitions

5.0. **Anti-virus software**: Software used to prevent, detect and remove malware. Anti-virus can also mean anti-malware and/or anti-spyware.

5.1. **Asset**: Any physical entity that can affect the confidentiality, availability and integrity of the organisation's information assets.

5.2. **Availability**: The accessibility and usability of an information asset upon demand by an authorised entity.

5.3. **Automated decision making:** Processing of information that results in decisions being made about Information Subjects without any review of the information being made by an individual.

5.4. **Beyond use**: Controls placed on Personal Information that it is no longer necessary for Lewis & Graves Partnership Ltd to keep where it is not reasonably feasible to delete the information. These controls must comply with guidance from the Information Commissioner's Office (see **Information Commissioner's Office Guidance on GDPR Compliance**).

5.5. **Computer systems**: A system of one or more computers and associated software, often with common storage, including servers, workstations, laptops, storage and networking equipment.

5.6. **Confidential information**: Any type of information that has been specified by the organisation's **Information Classification, Labelling and Handling Policy** as requiring protection through the application of cryptographic controls when it is stored or transferred electronically.

5.7. **Confidentiality**: The restrictions placed on the access or disclosure of an information asset.

5.8. **Controller:** A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of a set of Personal Information.

5.9. **Electronic communication facilities (ECF)**: Any asset that can be used to electronically transfer information.

5.10. **Electronic messages**: The electronic transfer of information by means such as email, texts, blogs, message boards and instant messaging.

5.11. **Equipment**: Any asset that can be used to electronically store and/or process information.

5.12. **High risk processing:** Processing of Personal Information (in particular using new technologies) that is likely to result in a high risk to the rights and freedoms of Information Subjects (see **Information Commissioner's Office Guidance on GDPR Compliance**).

5.13. **Identifiable Natural Person:** A natural person who can be identified directly or indirectly, in particular with reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

5.14. **Information asset**: Any information that has value to the organisation's stakeholders and requires protection.

5.15. **Information processing facility (IPF)**: Any network of assets that can be used to electronically store, process or transmit information.

5.16. **Information security critical supplier (ISCS)**: Any supplier of goods or services that as part of their scope of supply will potentially have unsupervised access to any of the organisation's premises**,** access to the one or more of the organisation's information assets**,** or provides software or hardware used in the organisation's information processing facilities or electronic communication facilities.

5.17. **Information security incident**: Any event that has a potentially negative impact on the confidentiality and/or integrity and/or availability of an information asset.

5.18. **Information subject**: An Identifiable Natural Person who has Personal Information that Lewis & Graves Partnership Ltd is the Controller of or is a Processor of on behalf of a Controller.

5.19. **Integrity**: The accuracy and completeness of an information asset.

5.20. **Mail serve**r: A system based on software and hardware that sends, receives and stores electronic mail.

5.21. **Malware**: Malicious software, such as viruses, trojans, worms, spyware, adware, macros, mail bombs and rootkits which are specifically designed to disrupt or damage a computer system.

5.22. **Mobile device**: Laptop computers, tablet computers, smart telephones, mobile telephones and any other handheld or portable devices capable of processing or transmitting information.

5.23. **Operating facility**: Any physical location containing assets owned by the organisation that the organisation controls, including buildings, offices, departments and locations affiliated with the organisation that are used to create, access, store or process any of the organisation's information assets.

5.24. **Personal Information**: Any information relating to an Identifiable Natural Person.

5.25. **Personal Information protection principles**: Principles that shall be applied in relation to all Personal Information as laid down in the Data Protection Act 2018, the General Data Protection Regulation (EU 2016/679) and any subsequent amendments.

5.26. **Processor:** A natural or legal person, public authority, agency or other body which processes Personal information on behalf of a Controller.

5.27. **Remote users**: Users accessing the organisation's assets at locations other than its operating facilities, such as home offices, shared locations, hotels and where users are travelling, including standalone access and remote connections to the organisation's information processing facilities.

5.28. **Restricted access**: Any physical location where access is restricted to named personnel only.

5.29. **Software**: All programs and operating information used by equipment, including those being developed in accordance with the customer's requirements for the user.

5.30. **Supply of goods and services agreement**: A legally binding contract between the organisation and a supplier for the supply of a defined scope of goods and services.

5.31. **Teleworker**: Any person that undertakes teleworking on behalf of the organisation.

5.32. **Teleworking**: The access, processing, and storage of information assets at locations that are not under the control of the organisation.

5.33. **User**: An individual or organisation that uses one or more of the organisation's assets, including software once it is post-General Availability (GA).

5.34. **Visual aids**: Any asset used to display information to the occupants of a room.

6.0. Associated Documents

6.0. All associated documents referred to in this policy are highlighted in bold and underlined.

7.0. Acceptable Use of Assets Policy

7.0. This sub-policy specifies the controls that need to be applied to:

7.0.1. Authorise the use of any asset owned by, or under the control of, the organisation; and

7.0.2. Minimise the risks to information security arising from the misuse or unauthorised use of the organisation's assets.

7.1. Use of Mobile Communication Devices (MCD) – phones, tablets, laptops

7.1.1. All users of MCDs must be authorised to do so in accordance with the organisation's **Access Control Policy**.

7.1.2. Users must only use assets to access and transfer information for which they have been authorised in accordance with the **Access Control Policy** and the **Information Classification, Labelling and Handling Policy**.

7.1.3. Users must apply extreme caution when opening email attachments received from unknown senders. If in doubt, please ask the IT Manager for advice. An extra layer of security (Minecraft) has been added to all dev ices, this will prevent suspicious/ malicious links from being opened from an unauthorised device.

7.1.4. Users must not:

- Disclose user IDs and personal passwords which give access to the organisation's assets unless authorised by the IT Manager.
- Allow any third party to access the organisation's MCDs.
- Use any access method other than the method provided to them by the organisation.
- Deliberately cause damage to any of the organisation's MCDs, including maliciously deleting, corrupting, or restricting access to the data contained therein.
- Deliberately introduce viruses or other harmful sources of malware into the organisation's MCDs.
- Deliberately access external sources that are not authorised and not related to the organisation's activities.
- Knowingly access, download or store materials from the internet that are illegal, immoral, unethical, or deemed to be indecent or gross in nature.
- Send unsolicited, unauthorised, or illegal materials to any internal or external recipient.
- Install, modify, delete, or remove software in a way that contravenes the **Use of Software Policy**.
- Download any electronic files whose size exceeds any guidance provided by the IT Manager. (5Mb)

- Assist or create a potential security breach or disruption to the organisation's MCDs in any way.
- Use any MCDs for any personal reasons, other than those authorised by the organisation.

7.1.5. Any user supplied equipment must be approved by the IT Manager for connection to any of the organisation's MCDs.

7.1.6. The organisation reserves the right to monitor the use of all MCDs

8.0. Access Control Policy

8.0. This sub-policy specifies the access controls that need to be applied to all information assets that contain information held by the organisation.

8.1. **Access to the information assets, operating facilities, and information processing facilities**

8.1.1. Access to information assets, operating facilities and information processing facilities must only be provided to individuals who need it to complete tasks specified in their **Job Description** or as instructed by either the IT Manager or General Manager/ Office Manager of the organisation.

8.1.2. All user access must be attributed to an identifiable person.

8.1.3. All users must ensure they do not save anything to the local drives on their computers and ensure nothing is saved to their desktops.

8.1.4. All unsupervised access to information assets, operating facilities and information processing facilities must be authorised by the person specified in, and recorded on, the **Access Control Register**.

8.1.5. The IT Manager is responsible for:

- Ensuring no single person can access, modify, or use the organisation's assets without authorisation.
- Authorising and recording the use of any software that might be capable of overriding this sub-policy.
- Authorising and recording access to any software source codes.
- Authorising and recording individual user access to information processing facilities, Mobile Communication Devices, operating facilities, and restricted access areas using an **Asset and Access Control Review Form**.
- Ensuring that individuals who enable and disable access to an organisation asset do not have access to any software that monitors the use of the asset.
- Ensuring that the access control for specific assets and information processing facilities meets the security requirements of each information asset owner.
- Regularly reviewing the logs of system administrator access and actions.

8.2. **Control of access to information processing facilities**

8.2.1. The IT Manager is responsible for:

- Arranging access with the General Manager/ Office Manager as part of the induction of new starters, and as part of any role changes within the organisation.
- Arranging the removal of access after notification from the General Manager/ Office Manager of leavers from the organisation and as part of any role changes.

- Ensuring access to any asset is not provided to an individual who has not received formal training in the **Information Security Policy**;
- Ensuring individual access privileges are reviewed upon a change of role or change in responsibilities.
- Recording the status of each user's access privileges in the **Access Control Register**;
- Ensuring redundant user access IDs are not issued to other users.
- Ensuring the immediate removal of all access rights of a user upon termination of their **Employment Contract**, or in the event of a security incident that relates to their access rights.

8.2.2. The IT Manager is responsible for:

- Responding in a timely manner to requests for the activation and deactivation of user account access made to them by the General Manager/ Office Manager.
- Configuring and reviewing user access to the organisation's assets and information processing facilities as specified in the **Access Control Register**.
- Removing any expired or unused accounts; email accounts will be maintained for a period of 12 months following which, the IT Manager will review that account.
- Testing that deactivated, deleted, and removed accounts are no longer accessible.
- Implementing access control systems and mechanisms for the organisation's assets and information processing facilities as directed by the General Manager/ Office Manager.
- Logging and monitoring all access to the organisation's assets and information processing facilities and providing access logs where requested to do so.
- Ensuring that access log files cannot be edited or deleted.

8.2.3. Any password rules and user security controls implemented must satisfy the following criteria:

- Passwords must be at least 8 characters in length.
- Passwords must be a combination of at least 1 upper case and at least 2 numbers.
- Passwords must automatically expire every 365 days.
- Historic passwords cannot be repeated.
- The IT Manager is responsible to change passwords on initial access or if access needs to be re-established for any reason.

- Passwords must be obscured on any access point that displays them, typically marked with an asterisk.
- Password files or data must be stored in encrypted secure areas and encrypted whilst transferred.
- All displays must have a timeout of 5 minutes or less where the user is prompted to enter a password to access the system.

8.2.4. The IT Manager is responsible for:

- Granting permanent or temporary access to restricted areas.
- Reviewing access to restricted areas every 365 days (internal access) and (30 days for external access) authorising changes where required.
- Leading and providing support to incident investigations where required.

8.2.5. All access requests to restricted areas must be made in writing and, as a minimum, include the following information:

- Reason for access.
- Areas of access required.
- Start and finish date (if permanent please state this).
- Line manager's approval (in writing).
- Any specific requirements, including restrictions and limitations of access.

8.3. **Access to remote users**

8.3.1. All users must adhere to the **Physical and Environmental Security Policy**, **Mobile Devices Policy** and **Acceptable Use of Assets Policy** when using the organisation's assets in remote locations.

8.3.2. Remote access to the organisation's network and information processing facilities must:

- Only be provided to authorised users.
- Only be used with approved assets, in accordance with the **Acceptable Use of Assets Policy**, **Teleworking Policy** and **Mobile Devices Policy**.
- Access to cloud-based files is exclusively restricted to approved and managed users / groups with the exception of granted external use which a link can be sent via email for the external user to Read Only. External Links expire after 72 hours.

8.4. **Access to the organisation's operating facilities**

8.4.1. Access to the organisation's operating facilities must be authorised by the General Manager/ Office Manager.

8.4.2. Access to the organisation's operating facilities will be processed and granted by the General Manager/ Office Manager

8.4.3. Access controls must be implemented at all the organisation's operating facilities and must be:

- Appropriate and proportionate to the area under control.
- Updated at set intervals to prevent the transfer of access methods to unauthorised persons and third parties.
- Monitored and logged for security purposes.

8.4.4. All employees are responsible for:

- Strictly adhering to the access controls for each location.
- Not tailgating or allowing tailgating through any secure access door.
- Not forcibly opening doors and other access controls.
- Not deliberately holding open a controlled access door by wedging, latching, or placing an item against it.
- Promptly reporting any problems relating to access controls to the General Manager/ Office Manager.
- Accompanying visitors that are in their care at all times, and not allowing them to enter any unauthorised location.
- Immediately reporting to the General Manager/ Office Manager and challenging, if confident and safe to do so, any person who is suspected of being in an area that they are not authorised to be in.

8.4.5. Authorisation must be granted by the General Manager/ Office Manager to hold open a controlled access door for longer than the time required for an individual to enter or exit the area.

8.5. **Visitors and suppliers**

8.5.1. All visitors must:

- Sign in at reception.
- Be accompanied by a member of the organisation's staff at all times.
- Not be allowed access to any restricted areas without the relevant authorisation to do so.
- Display the visitor's pass provided to them at reception.
- Return passes to reception when they leave the organisation's premises, even if for a limited period such as lunchtime.
- Not attempt to access any of the organisation's assets and information processing facilities or view any of the organisation's information without authorisation to do so.

8.5.2. All suppliers working in an operating facility must:

- Sign in at reception.
- Be managed and approved in accordance with the **Suppliers Policy**.
- Be appropriately inducted into the organisation by the relevant authority.

- Not access areas other than those identified as appropriate to perform the contracted tasks.
- Display a visitor's pass at all times.
- Return passes to reception when they leave the organisation's premises, even if for a limited period such as lunchtime.
- Immediately report any accidental breaches of this policy to the General Manager/ Office Manager.
- Not access or view any information that has not been provided as part of the contracted task.

8.5.3. **Remote access to customer networks**

8.6. **Keypad access to the Building**

8.6.1. The IT Manager is responsible for ensuring the code is only given to a limited number of senior Managers.

8.6.2. Keys to external security shutters will only be distributed to senior managers (security padlocks will be changed if a senior manager leaves the organisation).

9.0. Data Recovery Policy

9.0. This sub-policy specifies the controls that need to be applied to ensure that in the event of a loss of data/software the following steps will be taken. The risk to their confidentiality, availability and integrity is minimised.

9.1. Data recovery is managed through 2 Microsoft products SharePoint and OneDrive.

9.2. Metadata backups are kept for 14 days and can be recovered within a 5 minute window.

9.3. This link https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data describes how the data recovery process works.

9.4. **Attempt local fix.**

9.4.1. Repair of the device - this could be a software or operating system issue.

9.4.2. Restoration of backed up data - Data backed up via the cloud services can be restored

9.5. **Purchase replacement part**

9.5.1. If it is diagnoses as a non-repairable hardware issue, a new part (for example Hard Drive) will be replaced

9.6. **Purchase replacement device**

9.6.1. If multiple hardware issues exceed the cost of replacing the whole device. This would include for example a new PC or Laptop.

9.7. **Set up of replacement/new device.**

9.7.1. Set up of windows.

9.7.2. Sign in to give required access.

9.7.3. Install anti-virus.

9.7.4. Set up software applications.

9.7.5. Set up printers.

9.7.6. Set up cloud folders.

9.8. **If IT Manager is absent**

9.8.1 Contact Cobweb Solutions on 03333 234 934

10.0. Clear Desk and Clear Screen Policy

10.0. This sub-policy specifies the controls that need to be applied to minimise the risks to information security arising from unauthorised access to the organisation's information assets located on desks, visual aids, and display screens.

10.1. **Paper assets, visual aids, and portable storage media**

10.1.1. Information assets held on paper or portable storage media must be stored in cabinets and/or drawers, in accordance with the **Information Classification, Labelling and Handling Policy**, when not in immediate use and whenever the room they are being used in is vacated unless the room is vacated in accordance with the **Fire Evacuation Procedure**.

10.1.2. All information assets stored on visual aids should be removed from display immediately after used and before vacating the room in which they are held.

10.2. **Display screens Sleep mode**

10.2.1. Equipment that utilises display screens must have a screensaver enabled with password protection that activates automatically after 10 minutes of inactivity.

10.2.2. Users of equipment that utilises display screens must enable a screensaver whenever they leave the room in which they are held.

10.3. **Reproduction devices (printers, photocopiers, and scanners)**

10.3.1. Media used, or created using reproduction devices, must be removed from them immediately after use.

11.0. Communication Policy

Introduction

This policy sets out the approach that Lewis & Graves Partnership Ltd will adopt to ensure that effective communication remains an important part of the organisation's approach to delivering a range of services that are safe, environmentally friendly, and able to meet the needs of our customers.

Lewis & Graves Partnership Ltd recognise the importance that effective communication can have on its staff, clients, and other stakeholders. The following objectives have been developed to clearly signal what is important to the continued success of the organisation and keep a range of stakeholders informed of any key messages. Our Integrated Management System (IMS and ISMS) includes certification to ISO 9001, 14001, 45001 and 27001. Each Standard includes requirements to inform, involve and ensure participation by staff and relevant stakeholders in the development of the business, ensuring continuous improvement and working to improve the safety and well-being of staff.

Objectives

Raise Awareness of

- Key health & safety messages relevant to their role in the organisation
- The need to be environmentally responsible in the operation of our services
- The quality of service delivered to our customers and how it can be improved
- Key messages using a variety of means including posters, email, social media, meetings, brochures, manuals, and policies.
- Encourage the use of "non-standard" ways of communication including the use of pictures, photographs, translated documents and (where appropriate) interpreters.

Education & Training

- Promote and encourage staff to take advantage of new learning opportunities relevant to their role in the organisation.
- Work with clients to increase their environmental awareness and reduce waste.
- Publicise and promote new cleaning techniques, equipment, and cleaning products.

Minimise and mitigate risks to workers and the environment

- Ensure that the H & S Committee contributes to the development of a safe working environment and that its work is publicised.
- Regular reviews of accident statistic and near misses in order to learn and improve the organisation's safety record.
- Maintain and review the Innovations Log to ensure improvements are noted and monitored

Continuous Improvement

- Encourage innovation and ways of increasing efficiency or productivity.
- Identify areas for improvement using evidence from audits, inspections, and examples of best practice elsewhere.
- Encourage feedback from clients and stakeholders on a range of issues including our quality, environmental and H&S performance

Communication with third parties

- Any enquiries received from third parties relating to information security or the organisations or ISMS must be immediately referred to the IT Manager or, in their absence, the General Manager/Office Managers.
- Any information exchanged with third parties must be done in accordance with the **Information Classification, Labelling and Handling Policy** and the **Control of Documented Information Procedure**.
- Supply of information about the organisation's ISMS, including policies, procedures and specific control measures employed must be approved by the IT Manager.

A documented Procedure (5) describes how communication will be managed across the organisation. The Procedure sets out what will be communicated, when, to whom and how.

Finally, records will be maintained to ensure that the organisation is able to evidence its approach to communication and performance against the objectives described above.

12.0. Cryptographic Controls Policy (Sending Confidential Files)

12.0. This sub-policy explains how confidential information will be shared or sent

12.1. **General principles use**

12.1.1. The organisation's computer systems PC's, tablets, phones and laptops) must be protected to prevent unauthorised use or access by applying a level of protection to sensitive or critical information which is proportionate to the level of business risk.

12.1.2. All removable media, including memory sticks, must be protected by encryption.

12.1.3. Mobile devices Laptops, tablets and phones hard drives must be encrypted.

12.1.4. Mobile devices must be protected by passwords or PIN codes.

12.1.5. Emails must be encrypted whenever confidential information is contained or attached. Confidential information includes for example:-

- HR files containing names, NI numbers, addresses and other identifiable information
- Financial information
- Accident reports

12.1.6. The organisation's email system uses something called *BitLocker* for all mailbox data, the BitLocker configuration is described in BitLocker for Encryption. The Bitlocker system encrypts all mailbox data at the mailbox level. In addition Microsoft 365 supports **Customer Key**, Customer Key is a Microsoft-managed key. This method of encryption provides increased protection not afforded by BitLocker because it provides separation of server administrators and the cryptographic keys necessary for decryption of data, and because the encryption is applied directly to the data (in contrast with BitLocker, which applies encryption at the logical disk volume) any customer data copied from an Exchange server remains encrypted. The scope for Exchange Online service encryption is customer data that is stored at rest within Exchange Online. (Skype for Business stores nearly all user-generated content within the user's Exchange Online mailbox and therefore inherits the service encryption feature of Exchange Online.)

12.1.7. Attachments to emails must be encrypted whenever confidential information is contained.

12.1.8. Confidential information is sent via a secure Share Link via Office 365 cloud services, which gives access to that specific recipient with Read Only Access . An additional layer of protection is that the document is password protected (Eg Excel document) and the password is sent separately in another email.

12.1.9. All customer files in SharePoint Online are protected by unique, per-file keys that are always exclusive to a single tenant. The keys are either created and managed by the SharePoint Online service, or when Customer Key is used, created, and managed by customers. When a file is uploaded, encryption is performed by SharePoint Online within the context of the upload request, before being sent to Azure storage. When a file is downloaded, SharePoint

Online retrieves the encrypted customer data from Azure storage based on the unique document identifier and decrypts the customer data before sending it to the user. Azure storage has no ability to decrypt, or even identify or understand the customer data. All encryption and decryption happen in the same systems that enforce tenant isolation, which are Azure Active Directory and SharePoint Online.

Several workloads in Microsoft 365 store data in SharePoint Online, including Microsoft Teams, which stores all files in SharePoint Online, and OneDrive for Business, which uses SharePoint Online for its storage. All customer data stored in SharePoint Online is encrypted (with one or more AES 256-bit keys) and distributed across the datacenter as follows.

12.2 Encryption of data in transit

12.2.1 Confidential information in transit must always be encrypted. Data, which is already in the public domain, or would be of no adverse significance if it were to be so, may be sent unencrypted.

12.3 Key management Not Applicable

12.4 Encryption for information transferred outside the UK Not Applicable

12.5 Avoiding adverse impacts from encryption Not Applicable

13.0. Information Classification, Labelling and Handling Policy

Lewis & Graves are working towards a "paperless" office environment in order to increase information security and assist with our drive to protect the environment by minimising paper usage. Going forward documents will be designed to be used using a PC, mobile phone or tablet device, enabling electronic storage. Legacy forms and documents held in paper form will be managed and stored in a form that protects personal and confidential information.

13.0. This sub-policy specifies the labelling, storage, copying and distribution controls that need to be applied to all information assets that are processed and stored by the organisation. An **Information asset**: can be described as any information that has value to the organisation's stakeholders and requires protection.

13.1. **Classification**

13.1.1. It is the responsibility of the Compliance Manager to maintain the **I**nformation Classification, Labelling and Handling Rules contained in the **Control of Documented Information Procedure** to ensure that:

- Information assets can be easily classified, and that classification considers their value, criticality, legal requirements and sensitivity to unauthorised disclosure or modification.
- The rules can be applied practically by all information asset owners, employees and third parties with whom the organisation exchanges or provides access to information assets.

13.2. **Labelling**

13.2.1. Upon creation or receipt from a third party, all information assets must be labelled in accordance with the **Control of Documented Information Procedure (Appendix C)**.

13.2.2. Whenever an information asset is modified, consideration must be given as to whether the labelling applied to it should be changed.

13.2.3. Documents that are either confidential or sensitive will be labelled as "Confidential "or "highly confidential"

13.3. **Copying**

13.3.1. The copying of all information assets should be avoided wherever possible. Where copying is necessary (i.e., to comply with the **Backup Policy**), copying must be done in accordance with **Control of Documented Information Procedure (Appendix C)**.

13.4. **Distribution**

13.4.1. Information assets should only be distributed:

- To comply with client requirements.
- To comply with legal requirements.
- On a need-to-know basis.

13.4.2. Where distribution is necessary, it must be done in accordance with **Control of Documented Information Procedure (Appendix C)**.

13.5. **Destruction**

13.5.1. Destruction of an information asset must be done in accordance with the **Control of Documented Information Procedure**.

13.0. Mobile Devices Policy

13.0. This sub-policy specifies the controls that need to be applied to:

13.0.1. Control the use of any mobile devices owned by, or under the control of Lewis and Graves Partnership Ltd

13.0.2. Minimise the risks to information security arising from the misuse or unauthorised use of mobile devices.

13.1. **Issuing of mobile devices**

13.1.1. The issue of any mobile device to a user must be authorised by the General Manager/ Office Manager and recorded on the Assets Register.

13.2. **Use of mobile devices**

13.2.1. All users of mobile devices must comply with the **Acceptable Use of Assets Policy**, **Clear Desk and Clear Screen Policy**, **Data Recovery Policy**, **Teleworking Policy,** and the **Use of Software Policy**.

13.2.2. Mobile devices must only be used in connection with authorised business use, Devices can be used for personal use as long as company data is not compromised.

13.2.3. A mobile device must only be used by the user to whom it was supplied. Users must not allow a mobile device issued to them to be used by any other individuals including other employees, suppliers, friends, associates, or relatives.

13.2.4. In an emergency situation, a user may allow an individual to make a supervised call from a mobile device.

13.2.5. Users must immediately notify the General Manager/ Office Manager and the IT Manager if a mobile device is known or suspected to be lost or stolen.

13.2.6. Mobile devices must not be used or stored in environments or areas where there is a reasonable risk of them becoming damaged by impact, water ingress, extreme temperatures, or electromagnetic fields.

13.2.7. When not in use, mobile devices must be stored securely.

13.2.8. When mobile devices are taken away from buildings controlled by the organisation, users must ensure that they take adequate precautions at all times to protect the equipment against theft or accidental damage.

13.2.9. When transporting mobile devices, care should be taken not to draw attention to their existence to minimise the likelihood of street crime.

13.2.10. Laptops should only be transported in the bags or cases with which they were supplied or other appropriate bag holders.

13.2.11. Mobile devices must be carried as hand luggage when travelling.

13.2.12. Mobile devices must not be left unattended at any time in a vehicle or public place.

13.2.13. Mobile devices must always be protected from unauthorised use by an access password in accordance with the **Access Control Policy**.

13.2.14. Mobile devices must not be used to store passwords, safe/door combinations, or classified, sensitive or proprietary information unless accessed by second layer of security i.e Biometric

13.2.15. Users who have a device are expected to update their devices when prompted to do so when alerts and notifications come up. If you have any problems, you can contact the IT Manger.

13.3. **Return of mobile devices**

13.3.1. Upon request by the General Manager/ Office Manager, termination of contract or change of role, a user must return any mobile devices they have been issued with to the General Manager/ Office Manager or the Operations Manager

13.3.2. All mobile devices must be returned to the General Manager/ Office Manager who then passes it onto the IT Manager who then passes the information to the Compliance Administrator who will record the details in the Asset Register.

15.0. Physical and Environmental Security Policy

15.0. This sub-policy specifies the controls that need to be applied to all offices and assets located at them to:

15.0.1. Protect the organisation's assets from physical and environmental threats.

15.0.2. Reduce the risk of damage, loss, and theft to the organisation's assets;

15.0.3. Reduce the risk of unauthorised access to the organisation's offices.

15.1. **Physical protection of Lewis and Graves Offices**

15.1.1. Using appropriate methods, all the organisation's offices must be secured at all times to prevent unauthorised access.

15.1.2. All offices are protected by an intruder alarm system that is remotely monitored by The IT Manager.

15.1.3. **Burglary Alarm**

When the Alarm is triggered, the main operating office telephones the key holders to check if accidental or legitimate. The key holders that will be telephoned are as follows:

Tracey Parker – General Manager

Nick Jones – IT Manager

James Abbott – Senior Operations Director

Mark Graves - Director

Keith Lewis - Director

Jason King – Sales Manager

David Cowley – Regional Manager (Wandsworth)

If the alarm is deemed to be false, then the system alarms can be switch off. If it is deemed to be a legitimate break-in then the Police are automatically notified.

15.1.4. All external windows and doors must be kept shut and always locked unless authorised by the General Manager/ Office Manager.

15.1.5. Fire doors must not be blocked, chained, or left open.

15.2. **Environmental protection of offices**

15.2.1. All the environmental vulnerabilities and controls associated with the organisation's offices are identified in the **Asset and Risk Assessment Register**.

15.2.2. All relevant offices are protected by suitable fire alarm systems and have a fire evacuation procedure in place.

15.2.3. **Fire Alarm**

Touch points tested one a month by L&G staff.

Smoke detectors at Head Office are tested every 6 months by Shipman Security Systems. Wandsworth Office smoke detectors are tested by Ajax.

Both Burglary and fire alarm systems are serviced and maintained by Shipman Security Systems at Head Office, Both Burglary and fire alarm systems are serviced and maintained by Energex at Wandsworth Office.

15.2.4. All systems that need to be maintained in a temperature-controlled environment must be suitably located where air conditioning facilities are adequately maintained to ensure reliability.

15.3. **Protection of assets at offices**

15.3.1. All cable/wiring locations must be appropriately secured to prevent interception of data and damage to the network infrastructure.

15.3.2. All hard copy files must be stored in cabinets in accordance with the **Clear Desk and Clear Screen Policy** and the **Information Classification, Labelling and Classification Policy**.

15.3.3. All assets must be maintained in accordance with manufacturers and suppliers' recommendations or as identified from an **Improvement Log**. Maintenance requirements and their status will be recorded in the **Equipment and Maintenance Register**.

15.3.4. All areas designated as restricted access in the **Access Control Policy** must be clearly signposted at all entrance points to them. Entrances to these areas must be physically controlled at all times to prevent access by non-authorised personnel.

16.0. Protection from Malware Policy

16.0. This sub-policy specifies the controls that need to be applied to all computer systems and the mobile devices that can connect to the organisation's offices to protect them against malware threats from sources such as viruses and spyware applications.

16.1. **Installation of anti-virus software on computer systems and mobile devices**

16.1.1. It is the responsibility of the IT Manager to ensure that effective anti-virus software is installed and appropriately updated on all computer systems and mobile devices that have access to Lewis and Graves offices and store and transmit information assets, regardless of whether the organisation actively manages and maintains them.

16.1.2. All computer systems and mobile devices must not be used or handed over to a user unless they have up-to-date and operational anti-virus software installed.

16.1.3. All anti-virus software installed must have real-time scanning protection to files and applications running on the computer system or mobile device. The scanning must automatically assess the threat posed by any electronic files or software code downloaded onto a computer system or mobile device.

16.1.4. All anti-virus software must be configured to ensure it can detect, remove, and protect against all known types of malwares.

16.1.5. All anti-virus software must be configured to automatically start on device power-up and to continuously run for the duration that the computer system or mobile device is powered.

16.1.6. All anti-virus software must be configured to run automatic updates provided by the anti-virus software supplier.

16.1.7. All anti-virus software must be configured to conduct periodic scans of the computer system or mobile device on which it is installed.

16.1.8. All anti-virus software must be configured to generate log files, and to store these log files either locally on the computer system or mobile device or centrally on an organisation-wide anti-virus server (if applicable). All logs must be kept for a minimum of 30 days.

16.2. **Installation of anti-virus software on mail servers Not Applicable**

16.3. **Other processes, systems, and tools to deter malware.**

16.3.1. All computer systems and mobile devices must run the organisation's approved operating system at its latest supported version with all relevant updates and patches installed.

16.3.2. Web filtering must be implemented to reduce the potential access to websites that may contain malicious code.

16.4. **Requirements of users**

16.4.1. Any activity intended to create and/or distribute malware on an information processing facility, computer system or mobile device is strictly prohibited.

16.4.2. All users must not in any way interfere with the anti-virus software installed on any computer system or mobile device.

16.4.3. All users must immediately report any issues, or suspected issues relating to malware and any anti-virus warnings and alerts communicated to them from a computer system or mobile device.

16.4.4. All users must check the authenticity of attachments/software to be installed from internet sources.

16.4.5. Users must not install applications that arrive on unsolicited media.

16.4.6. Users must seek advice from the IT Manager if their computer system or mobile device requests them to install or update software such as Java and ActiveX.

16.4.7. Users must seek authorisation to install any previously unauthorised software.

17.0. Protection of Personal Information Policy

17.0. This sub-policy specifies the controls that need to be applied to the storage, processing and dissemination of Personal Information that is accessed, stored, or processed by the organisation to ensure that Lewis & Graves Partnership Ltd complies with and can demonstrate compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

17.1. **Data Protection Officer**

17.1.1. Lewis & Graves Partnership Ltd have appointed a Data Protection Officer whose contact details are published on the company's website and communicated to the Information Commissioner's Office.

17.1.2. The appointed Data Protection Office will:

- Report directly to Top Management.
- Be involved properly and in a timely manner, in all issues which relate to the protection of Personal Information.
- Have the full support of Top Management in performing their tasks.
- Be provided with all resources necessary to carry out the tasks required by the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).
- Be provided with all the resources necessary to maintain their expert knowledge.
- Have unlimited access to Personal Information processing operations.
- Not receive any instructions from Top Management regarding the exercise of the tasks required by the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).
- Not be dismissed or penalised by the Top Management for performing tasks and duties required of them by the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).
- Not undertake any other tasks and duties that result in a conflict of interest.

17.1.3. It is the responsibility of the Data Protection Officer to:

- Inform and advise Top Management, employees and any suppliers who undertake processing of Personal Information on behalf of Lewis & Graves Partnership Ltd, of their obligations in regard to this policy and the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).
- Monitor Lewis & Graves Partnership Ltd.'s compliance with this policy, the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

- Ensure all relevant employees have appropriate training with regards to processing of Personal Information.
- Act as a contact point for the Information Commissioner's Office on issues relating to the processing of Personal Information.

17.2. **Application of the Personal Information protection principles**

17.2.1. The following principles must be applied and compliance with them demonstrated in relation to all Personal Information that is accessed, stored, or processed by employees, and employers or suppliers, while they are accessing or processing the Lewis & Graves Partnership's information assets and any Personal Information that Lewis & Graves Partnership is the Controller of or processing on behalf of another Controller:

- Personal information shall be processed lawfully, fairly and in a transparent manner.
- Personal information shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.
- Any Personal Information collected shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Any Personal information processed shall be accurate, kept up to date (where necessary) and every reasonable step is taken to ensure that Personal Information that is inaccurate with regards to the purposes for which it is processed is erased or rectified without delay.
- Personal information shall not be kept in form that permits identification of Information Subjects for longer than is necessary for purposes for the which the personal information is processed (Personal Information may be put Beyond Use where deletion is not reasonably feasible).
- Appropriate technical and organisational measures shall be taken to ensure appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage.

17.2.2. All processes and operations that involve the processing of Personal Information must be designed to ensure that these principles can be achieved and are applied. Where any changes are required to Lewis & Graves Partnership's Assets that impact on the processing of Personal Information, the **Change Control Procedure** must be applied.

17.3. **Registration with the Information Commissioner**

17.3.1. It is the responsibility of the General Manager to ensure that the appropriate registration is maintained with the Information Commissioner.

17.4. **Personal Information Processing Register**

17.4.1. It is the responsibility of General Manager to ensure that a **Personal Information Processing Register** is maintained that contains information on

- All Personal Information that Lewis & Graves Partnership is the Controller of regardless of whether it is processed by Lewis & Graves Partnership or by a Processor engaged b Lewis & Graves Partnership.
- All Personal Information that Lewis & Graves Partnership is a Processor of on behalf a Controller or other Processor.
- The types of Information Subjects that the Personal Information relates to, the limit of the information collected and the source that it is obtained from.
- The reason the processing is undertaken and the legal grounds for doing so.
- The types of processing employed, and the methods and technologies used.
- The details of any Processers used (where Lewis & Graves Partnership is the Controller) or direct Sub-Processors used (where Lewis & Graves Partnership is the Processor).
- The country or region where the Personal Information is processed and stored.
- All recipients of the Personal Information.
- The period for which the Personal Information is retained and the justification for doing so.
- Whether any Automated Processing is undertaken.
- Whether the Personal Information falls into a Special Category and if so, the processing justification offered by Article 9 of the General Data Protection Regulation (EU 2016/679) that applies.
- Whether the Personal Information is transferred in any way outside of the EU and if so the countries/territories/organisations it is transferred to.

17.5. **Consent to Process Personal Information**

17.5.1. Where Lewis & Graves Partnership's is a Controller of Personal Information and it undertakes processing of Personal Information requiring the consent of the Information Subject, a record of the consent must be obtained from the Information Subjects using a **Privacy Notice + Consent Opt-in Form**.

17.6. **Processing of Personal Information obtained from an Information Subject**

17.6.1. Where Lewis & Graves Partnership Ltd has collected personal data directly from an Information Subject, they must be provided with a **Privacy Notice**

that contains at least the following information who consent to the processing of their Personal Information of the name and contact details of Lewis & Graves's Information Security Manager/Data Protection Officer.

- The scope and legal justification of processing that will be undertaken with the information they provide.
- Where the legal justification for processing the Personal Information is the Controller's legitimate interest, details of the legitimate interest.
- Where the legal justification for Processing the Personal Information is that the Information Subject has consented to the processing, the existence of a right to withdraw consent at any time, without affecting the lawfulness of the processing carried out prior to the withdrawal.
- The categories of recipients who will have access to their Personal Information.
- The time period for which their information will be stored or the criteria that will be applied to determine the time period.
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.
- Any planned transfers of their information to a third party, country or international organisation and information on the safeguards being applied and the means by which the Information Subject can obtain a copy of them or where they are available.
- Whether any automated decision-making will be applied to their information and if so, the logic that will be applied and the envisaged consequences for them.
- Whether Lewis & Graves Partnership is a joint Controller of the information and if so and overview of the agreement in place with other joint Controllers.
- Their rights to:
    - request access to their information
    - request corrections be made to their information
    - request their information be deleted
    - request that processing of their information is restricted
    - request their information be transferred to another Controller
    - lodge a complaint with the Information Commissioner

- and the means by which they can notify Lewis & Graves Partnership Ltd to exercise one or more of these rights.

17.7. **Processing of Personal Information obtained from third parties**

17.7.1. Where Lewis & Graves Partnership Ltd is a Controller of Personal Information and it undertakes processing of Personal Information obtained from a third party (i.e., not directly from the Information Subjects it relates to) then unless:

- The Information Subject already has the information that Lewis & Graves Partnership Ltd has obtained; or
- The collection or disclosure of the information is authorised or required by EU or UK law; or
- The disclosure of the information is restricted by due to the obligation of a professional body that has provided it or a requirement of EU or UK law.
- It would require a disproportionate effort to provide the information.

Lewis & Graves Partnership Ltd will provide the following information to Information Subjects about whom the Personal Information relates to:

- The name and contact details of Lewis & Graves Partnership Ltd.'s Information Security Manager/Data Protection Officer.
- The scope and legal justification of processing that will be undertaken with the information they provide.
- The categories of information that will be processed.
- The categories of recipients who will have access to their Personal Information.
- The source of the Personal Information and whether that source was publicly available.
- The time period for which their information will be stored or the criteria that will be applied to determine the time period.
- Where the legal justification for processing the Personal Information is the Controller's legitimate interest, details of the legitimate interest.
- Where the legal justification for Processing the Personal Information is that the Information Subject has consented to the processing, the existence of a right to withdraw consent at any time, without affecting the lawfulness of the processing carried out prior to the withdrawal.
- Any planned transfers of their information to a third party, country or international organisation and information on the safeguards

being applied and the means by which the Information Subject can obtain a copy of them or where they are available.

- Whether any automated decision-making will the applied to their information and if so, the logic that will be applied and the envisaged consequences for them.
- Whether Lewis & Graves Partnership Ltd is a joint Controller of the information and if so and overview of the agreement in place with other joint Controllers.
- Their rights to:
- request access to their information
    - request corrections be made to their information
    - request their information be deleted
    - request that processing of their information is restricted
    - request their information be transferred to another Controller
    - request to not be subject to a decision based solely on Automated Processing.
    - lodge a complaint with the Information Commissioner

    and the means by which they can notify Lewis & Graves Partnership Ltd to exercise one or more of these rights.

This information will be provided to Information Subjects either within one month of Lewis & Graves Partnership Ltd obtaining the information or at the time of first communicating with the Information Subject (whichever is the soonest).

17.8. **Accessing, processing and storage of Personal Information**

17.8.1. The General Manager must ensure that appropriate physical and technical controls are in place to:

- Protect the confidentiality, integrity, and availability of all Personal Information.
- Prevent unlawful processing of Personal Information.

17.8.2. Personal Information should be accessed, processed, and stored only to:

- Fulfil the needs of customers.
- Comply with legal requirements.
- Enable the effective implementation of the organisation's ISMS.

17.8.3. Personal Information should be accessed, processed, and stored in accordance with this policy, the specifications detailed in the **Personal**

Information Processing Register and the **Information Classification, Labelling and Handling Policy**.

17.8.4. Access to Personal Information must be provided in accordance with the **Access Control Policy**.

17.9. **Requests by Information Subjects to exercise their rights and freedoms**

For all Personal Information that Lewis & Graves Partnership Ltd is the Controller of:

17.9.1. All requests by Information Subjects whose Personal Information are processed by Lewis & Graves Partnership Ltd to exercise their rights and freedoms under the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679) will be managed in accordance with the **Handling of Personal Information Requests Procedure**.

17.9.2. Any information that needs to be provided to Information Subjects who submit requests will be provided in a concise, transparent, intelligent, and easily accessible form, using clear and plain language.

17.9.3. Any information requested by Information Subjects in the relation to any of their Personal Information processed by Lewis & Graves Partnership Ltd that Lewis & Graves Partnership Ltd is legally obliged to provide, will be provided free of charge unless the request if manifestly unfounded or excessive, in which case Lewis & Graves Partnership Ltd may change a reasonable fee for providing the information of refuse to act on the request.

17.9.4. Where the request covers the deletion of information that has been made public then Lewis & Graves Partnership Ltd will take all reasonable steps possible to inform other Controllers who are processing the information to delete any copy of the information that they hold or any links they have to the information.

17.10. **Transferring Personal Information**

17.10.1. Any transfer of Personal Information to a third party must be carried out under a written agreement, setting out the scope and limits of the sharing and in accordance with the **Information Classification, Labelling and Handling Policy**.

17.10.2. In the event that Lewis & Graves Partnership Ltd needs to transfer Personal Information to a EU country or an international organisation then:

- Relevant **Privacy Notices** needs to be updated to reflect this.
- The Information Subjects affected must be informed before the transfer takes place and provided with information regarding the safeguards that Lewis & Graves Partnership Ltd will ensure are in place.

17.11 Compliance and Controls Assessments

17.11.1 To ensure that:

- All controls employed to protect Personal Information is controlled or processed by Lewis & Graves Partnership Ltd are maintained and effective.
- Lewis & Graves Partnership Ltd complies with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

a schedule of audits will be completed as detailed in the **Internal Audit Schedule** and in accordance with the **Internal Audit Procedure**.

17.12 Arrangements with Joint Controllers

17.12.1 Where Lewis & Graves Partnership Ltd is a joint Controller of any Personal Information then a **Joint Controller Agreement** (or an equivalent agreement) will be implemented with any joint Controllers.

17.13 Arrangements with Controllers

Where Lewis & Graves Partnership Ltd undertakes processing on behalf of a Controller

17.13.1 A **Personal Data Processing Contract** will be (or an equivalent agreement) will be implemented with any Processors.

17.13.2 No processing of information provided by the Controller will be undertaken without an explicit instruction from them.

17.14 Arrangements with Processors

Where Lewis & Graves Partnership Ltd uses a supplier to undertake processing on its behalf:

17.14.1 A **Personal Data Processing Contract** will be (or an equivalent agreement) will be implemented with any Processors.

17.14.2 The **Change Management Procedure** shall be applied before changing supplier or taking on a new supplier and any applicable Controllers will be notified in writing of the change and provided with an opportunity to object to the change.

17.14.3 A **Personal Information Processor Assessment** will be completed to assess whether they can provide sufficient guarantees to implement appropriate control measures that will ensure the processing they undertake complies with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679) and protects the rights and freedoms on the Information Subjects whose information they process on behalf of Lewis & Graves Partnership Ltd.

17.14.4 An audit of a supplier's compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679 will be undertaken where:

- The information obtained from a **Personal Information Processor Assessment** raises doubts as to the adequacy of the guarantees provided by a Processor; or
- The supplier is undertaking High Risk Processing; or
- An information security incident occurs that has a significant impact on the confidentiality or integrity or availability of any Personal Information and following an investigation of the root cause of the incident, the controls and processes employed by the supplier are identified as having been a contributing factor.

The audit will be completed using the **Active Legal by the Compliance Manager.**

17.15 High Risk Processing

17.15.1 A data impact assessment must be completed for any High-Risk Processing of Personal Information that Lewis & Graves Partnership Ltd is a Controller of before any such processing is started.

17.15.2 The results of the data impact assessment must be recorded in the **Personal Information Processing Register**.

17.15.3 If a data impact assessment indicates that the processing would result in a high risk to the rights and freedoms of the Information Subjects whose Personal Information is being processed, then the General Manager must consult with the Information Commissioner's office before any processing is started.

17.16 Personal Information Breaches

17.16.1 In the event of a Security Incident that compromises the confidentiality, integrity or availability of any Personal Information actions shall be taken and records maintained in accordance with the **Security Incident Management Procedure**.

18.0. Suppliers Policy

18.1.1 This sub-policy specifies the controls that need to be applied to all suppliers who can compromise the security of the organization's information assets.

18.1.2 This sub-policy does not apply to services supplied by individuals under the terms of an **Employment Contract** issued by the organization.

18.1.3 Lewis and Graves Partnership Limited use a limited number of security critical suppliers, most of whom are national companies. Lewis and Graves Partnership Limited is restricted in its ability to force these organizations to operate on its own terms and conditions. These organizations will have their own terms of conditions contract which includes responsibility to manage any data supplied to it in accordance with the Data Protection Act 1998 and any other relevant legislation.

18.2 **Information security critical suppliers (ISCS)**

18.3 The use of all ISCS must be approved by the General Manager/ Office Manager.

18.4 This use of all ISCS who undertake processing of Personal Information on behalf of Lewis & Graves Partnership Ltd must done in accordance with the **Protection of Personal Information Policy** as far as is reasonably practicable.

18.5 Up-to-date records relating to the status of information about ISCS security controls, certifications and key personnel must be maintained in the **List of Interested Parties Register**.

18.6 All information security risks identified that relate to the use of ISCS must be assessed and recorded in the **Asset and Risk Assessment Register** in accordance with the **Information Asset and Risk Management Procedure**.

18.7 ISCSs must not deliver services that are not covered within the scope of a current terms and conditions with that organization:

- The scope of goods and services supplied by the ISCS covered by the agreement.
- The obligations of the ISCS to protect the organisation's information assets in respect of availability, integrity, and confidentiality.
- The obligations of the ISCS to comply with the organisation's **Information Security Policy** as far as is reasonably practicable and relevant processes, policies, and procedures in its ISMS, including acknowledgement of documents supplied by the organisation.
- The minimum information security controls implemented and maintained by the ISCS to protect the organisation's information assets and the arrangements for monitoring their effectiveness.
- The arrangements for reporting and managing security incidents in line with the organization's terms and conditions and any requirements of the Information Commissioner Office.
- The contact names of the persons employed by the organisation and ISCS with responsibility for information security.

- The defect resolution and conflict resolution processes contained within the organization's terms and conditions contract with Lewis and Graves Partnership Limited.

18.8 The information security controls detailed above should include the following considerations:

- Subcontracting of the supply of goods and services by the ISCS to third parties which will not be unreasonably withheld by Lewis and Graves Partnership Limited.
- Access control to the organisation's assets by ISCS employees and subcontractors.
- Resilience, recovery, and contingency arrangements to ensure the availability of any assets including any information processing facilities provided by the ISCS and/or the organisation.
- Accuracy and completeness controls to ensure the integrity of the assets, information or information processing equipment/facilities provided by the ISCS and/or the organisation.
- Processes and/or procedures for transferring information and/or information processing facilities between the ISCS, the organisation and other third parties.
- Any legal and regulatory requirements, including information protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met.

18.9 It is the responsibility of the General Manager to create and maintain the **List of Interested Parties Register**.

18.10 It is the responsibility of the General Manager to ensure that all ISCS suppliers are provided with up-to-date copies of the organization's policies and procedures that are relevant to them.

18.11 It is the responsibility of the General Manager to ensure that the information security controls specified in the terms and conditions of contracts with these suppliers (Banks, Insurance, Payroll, Pensions) are appropriate for the information they hold on behalf of Lewis and Graves Partnership Limited.

19. **Teleworking Policy**

This sub-policy specifies the controls that need to be applied to teleworking to minimize the risks to information security arising from the access, processing, and storage of information assets at locations that are not under the control of the organization.

19.1 **Teleworking authorization**

19.1.1 All teleworking must be approved by General Manager/ Office Manager.

19.1.2 The scope of a teleworker's teleworking must be defined to include:

- Authorised locations for teleworking, e.g. home, hotels, travelling etc.
- Mobile devices to be used.
- Access controls to the organisation's information
- Any specific controls to be applied, e.g. use of equipment by other individuals.

19.2. **Accessing the organization's information processing facilities from teleworking locations**

19.2.1 Teleworkers must comply with the **Access Control Policy**, **Acceptable Use of Assets Policy**, **Mobile Devices Policy,** and the **Protection from Malware Policy** when connecting to the organization's Cloud base information whilst teleworking.

19.2.2 Remote access to the organization's Cloud base information will be authorized by the IT Manager.

19.3 **Organization-provided equipment for teleworking**

19.3.1 Where equipment is provided to the teleworker for teleworking, the teleworker must comply with the **Acceptable Use of Assets Policy**, **Mobile Devices Policy** and **Use of Software Policy.**

19.4 **Use of teleworker-owned equipment for teleworking is prohibited**

20.0 Use of Software Policy

This sub-policy specifies the controls that need to be applied covering the use and installation of software on any assets owned by or under the control of the organization to minimize risks to information security arising from the misuse of software or the use of unauthorized or illegally obtained software.

20.1 **Use of software**

20.1.1 Software must only be used in connection with authorized business use.

20.1.2 Users of software must be authorized to so in accordance with the **Access Control Policy**.

20.1.3 Users must not make copies of any software provided by the organization without the express written consent of the software publisher and the organization.

20.2 **Installation of software**

20.2.1 Installation of software onto an PC/Mobile device must be authorized by the IT Manager and must be done in accordance with the **Change Control Procedure** and Mobile Devices Policy.

20.2.2 Users must not install, or in any way make use of, software from sources other than those provided by the organization unless authorized to do so by the IT Manager.

20.2.3 Any software installed must carry a valid license that covers the scope of use.

21.0 Policy Review

21.1 This policy and its sub-policies should be reviewed at least once per year or if significant changes occur that might affect its continuing suitability, adequacy and effectiveness.