CIBUS CAPITAL LLP: CIBUS CYBER SECURITY POLICY

This Summary is not exhaustive, supersedes any earlier procedures, is current as of the above date and may be varied or amended by management from time to time as circumstances dictate.

This document is confidential, provided for informational purposes only and is not legally binding on Cibus or any of its affiliates. Cibus accepts no responsibility to any third person in connection with, and no third person shall have any right to enforce, any performance or non-performance of any of the provisions of this document.

In no event shall this document constitute or be considered as advice or solicitation to invest in any specific investment or fund advised by Cibus or its affiliates, nor should this document be relied upon in making any investment decision. The information contained in this document shall not be considered as legal, tax or other advice.

This document is liable to change at any time, without notice.

1. INTRODUCTION

1.1 This policy applies to Cibus Capital LLP (the **"LLP"**) and its employees, contractors and third-party entities with access to the LLP's IT resources.

1.2 This policy outlines our organisation's approach to cyber security and data protection in alignment with the Financial Conduct Authority's regulatory expectations and the UK General Data Protection Regulation (UK GDPR).

1.3 This policy aims to protect the confidentiality, integrity, and availability of our systems and data while maintaining the trust of our clients, partners, and regulators.

1.4 This policy (the **"Policy"**) was adopted on 11 July 2025 and supersedes any earlier version of Cibus' Cyber Security Policy.

1.5 This Policy is reviewed annually and may be amended on an ad hoc basis if required.

2. BACKGROUND AND PURPOSE

2.1 This Policy outlines the principles, guidelines and procedures of the LLP to ensure the security and integrity of the LLP's information systems and data assets.

2.2 The purpose of this Policy is to:

(a) protect the confidentiality, integrity and availability of the LLP's information assets;

(b) prevent the unauthorised access, use, disclosure, modification or destruction of the LLP's data;

(c) ensure compliance with legal, regulatory and contractual requirements related to information security; and

(d) promote a culture of security awareness and accountability among all users of the LLP's IT resources.

3. ROLES AND RESPONSIBILITIES

3.1 The LLP's approach to cyber and data security is grounded in clear governance structures where the Management Board holds ultimate accountability for cyber risk management, with executive oversight delegated to the **Chief Information Security Officer (CISO)** and the **Data Protection Officer (DPO)**, where appointed. Senior managers are responsible for implementing appropriate controls within their areas, in line with the FCA's Senior Managers and Certification Regime (SM&CR).

3.2 **Chief Information Security Officer:** the LLP shall appoint a Chief Information Security Officer (CISO) of Data and Information Technology. The current CISO is Mr James Buist.

3.3 **Systems Administrator:** the LLP shall appoint a Systems Administrator for administering its data and information security. The current Systems Administrator is Mr James Buist.

3.4 **Data Protection Officer:** the LLP's Data Protection Officer is Jeremy Alun-Jones.

3.5 **IT Consultants:** the LLP uses a third-party consultant (James Buist) for technical matters.

4. WHAT WE ARE PROTECTING

4.1 The LLP conducts regular assessments to identify, evaluate, and manage cyber and data protection risks. These include threats to personal data processing, critical systems, and outsourced services. Where a project presents high risk to individuals' rights and freedoms, a formal Data Protection Impact Assessment (DPIA) is carried out in accordance with GDPR requirements.

4.2 It is the obligation of all users of the LLP's IT systems to protect the technology, information assets and confidential data of the LLP. Such technology and information assets include, but are not limited to, the following:

(a) computer hardware, CPU, disc, email, web, application servers, PC systems, application software, system software;

(b) system software including operating systems, database management systems and backup and restore software, communications protocols;

(c) application software including custom written software applications and commercial off-the-shelf software packages;

(d) communication networks including hardware, software, routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

5. THREATS TO SECURITY

5.1 The LLP's IT infrastructure is monitored continuously for suspicious or unauthorised activity. System logs are retained and reviewed to support both real-time incident detection and retrospective analysis. Monitoring extends to our outsourced services, in line with our responsibilities under the FCA's guidance on third-party risk. Here follows some of the key threats to the LLP's IT infrastructure.

Employees

5.2 One of the LLP's biggest security threats is its employees who may do damage to the LLP's systems either through incompetence or with malicious intent. The LLP layers its information technology security to compensate for employee threats. This includes the following procedures:

(a) only give out access rights to systems to appropriately senior staff and on a need-to-know basis;

(b) do not share accounts to access systems. Cibus' members/partners, staff should never share login information with co-workers or third parties;

(c) when any LLP employment or consultancy contract is terminated, or the staff member is suspended or otherwise disciplined, the LLP removes or limits access to the LLP's systems; and

(d) keeping detailed server access logs on computer activity.

Email Phishing

5.3 Phishing emails are more common now than ever and whilst the majority are filtered out through the spam filter built into Office 365 and the LLP's firewall, occasionally one will make it into a staff inbox.

5.4 The LLP's staff are trained to be able to recognise a phishing or 'clickbait' email and should be cautious when clicking on poorly explained links within emails.

5.5 Staff should always check the sender's email address before clicking on any links found within an email and if the sender is in any way unfamiliar, report it to the Compliance Department and IT consultants immediately by forwarding the suspicious email and any files but without clicking the links.

Malware

5.6 Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware.

5.7 It is a requirement that all staff laptops have up to date antivirus software installed on their work machines to mitigate this risk. If a staff member were to contract malware onto their machine, they are obliged to leave their laptop switched on and contact the IT consultants at their earliest convenience.

Amateur Hackers and Vandals

5.8 These people are the most common type of attackers on the internet. The probability of this sort of attack is extremely high and there is also likely to be a large number of these attacks (which are normally crimes of opportunity). These amateur hackers are scanning the internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favourite targets. Once they find a weakness, they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness, they are likely to move on to an easier target.

5.9 The LLP maintains firewalls and uses password logins as protection against this risk.

Criminal Hackers and Saboteurs

5.10 The probability of this type of attack against the LLP is low, but not impossible given the amount of sensitive information contained in databases. The LLP does not hold large amounts of retail client data, bank account details or sensitive or confidential public market information. If the objective of a would-be hacker is to gain large amounts of sensitive data then their efforts are better served elsewhere. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. These attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the relevant networks.

5.11 Whilst this is a remote threat for a business such as the LLP, the LLP maintains firewalls and uses password logins as a protection against this risk.

Incident Response

5.12 Cibus maintain a formal incident response plan that enables timely detection, investigation, and remediation of cyber incidents and data breaches. Where a personal data breach occurs, we assess the risk to individuals and notify the Information Commissioner's Office (ICO) within 72 hours when required. If there is a risk of serious harm, we inform affected individuals without undue delay. Where an incident is material, we inform the FCA in accordance with Principle 11.

5.13 Staff members experiencing a breach or that suspect a breach has occurred must cease interaction with the infected device and inform the IT Professionals employed by the LLP immediately.

6. USER RESPONSIBILITIES

6.1 This section establishes the LLP's usage policy for the LLP's computer systems, networks and information resources. This section of the Policy pertains to all users of the LLP's computer systems, networks, and information resources.

6.2 All users are expected to have knowledge of this Policy and are required to report violations to the Systems Administrator. Furthermore, all Cibus staff must conform to the Acceptable Use Policy set out below. The LLP has established the following user groups and defined the access privileges and responsibilities:

(a) **Department Users (LLP members and employees):** access to application and databases as required for job function. (RED and/or GREEN cleared)

(b) **System Administrators:** access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only.

(c) **Security Administrator:** highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.

(d) **System Analyst/Processor:** access to applications and databases as required for specific job function. Not authorised to access routers, firewalls, or other network devices.

(e) **Contractors/Consultants:** Access to applications and databases as required for specific job functions. Access to routers and security system only if required for job function. Knowledge of security policies and access to company information and systems must be approved in writing on a case-by-case basis by the Chief Information Officer and LLP Management Board. Access should be monitored and revoked on termination of the contractual relationship.

(f) **Other third parties and business partners:** access allowed to selected data rooms, and log-in portals only in connection with their relationship with Cibus.

(g) **General Public:** access is limited to information on the LLP's public website. The general public will not be allowed to access confidential information.

Acceptable Use

6.3 User accounts on the LLP's computer systems are to be used only for business of the LLP and not for personal activities. Unauthorised use of the LLP's system may be in violation of the law, may constitute theft and can be punishable in accordance with the LLP's Disciplinary Policy (as contained in the LLP's Staff Handbook).

6.4 All employees receive mandatory training on information security and data protection, including recognising phishing attempts, safeguarding personal data, and fulfilling individual responsibilities under UK GDPR. Specialist training is provided to all staff on an annual basis and refresher sessions are provided intermittently during the year.

6.5 The LLP's information technology users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their login IDs and passwords. Furthermore, the LLP's staff are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised persons outside the LLP and its affiliates.

6.6 The LLP's information technology users shall not:

(a) purposely engage in any activity with the intent to:

(i) harass other users;

(ii) degrade the performance of the system;

(iii) divert system resources for their own use; or

(iv) gain access to those parts of Cibus' systems for which they do not have authorisation.

(b) attach unauthorised devices to their PCs or workstations, unless they have received specific authorisation from their direct supervisor, a Partner and/or Cibus' Chief Information Officer or Systems Administrator;

(c) download unauthorised software from the internet onto their PCs or workstations.

6.7 The LLP's information technology users are required to report any weaknesses in the LLP's computer security and any incidents of misuse or violation of this policy to Cibus' Chief Information Officer or Systems Administrator.

Use of the Internet

6.8 The LLP provides internet access to users who are connected to the LLP's internal network in its London office. Users should obtain the relevant wi-fi access codes from the LLP's Security Administrator.

6.9 The internet is a business tool for the LLP. It is to be used for business-related purposes such as: communicating via electronic mail, video/audio calls with suppliers and business partners, obtaining useful business information, research and relevant technical and business topics.

6.10 **The LLP's internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for "chain letters" or any other purpose which is illegal or for personal gain. For further details please see the LLP's Staff Handbook.**

Monitoring Use of Computer Systems

6.11 The LLP has the right and capability to monitor electronic information created and/or communicated by persons using the LLP's computer systems and networks, including e-mail messages and usage of the internet.

6.12 Emails and documents created by the LLP's members and staff in connection with their employment are the intellectual technology and property of the LLP. It is not the LLP's current policy to continuously monitor all computer usage by members/partners, staff or other users of the LLP's computer systems and network.

However, users of the systems should be aware that the LLP may monitor usage, including, but not limited to, patterns of usage of the internet (e.g. site accessed, on-line length, time of day access), and users' electronic files and messages to the extent necessary to ensure that the internet and other electronic communications are being used in compliance with the law and with the LLP's internal policies.

7. ACCESS CONTROL

7.1 A fundamental component of this Policy is controlling access to the critical information resources that require protection from unauthorised disclosure or modification.

7.2 The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorised to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. Every member/partner or staff member's user account also has dual factor authentication enabled when logging into the secure portal. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

7.3 The default access level of all LLP staff member's user profiles is, 'Basic User Level Access' meaning that they have access to common share files and nothing else.

7.4 Folders, files or information that is deemed inappropriate or confidential for Basic User Level Access has its access restricted to certain groups of users based on sensitivity, need-to-know, access/editing rights, personnel confidentiality, and/or regulatory requirements. Access to these files is monitored and granted by System Administrator Level Users.

7.5 Administrators are:

(a) James Buist, the LLP's external IT consultant, Security Administrator;

(b) Fred Appleby, the LLP's in house IT specialist, System Administrator; and

(c) Computer Care, the LLP's third-party IT consultant, Security Administrator.

7.6 The LLP's Compliance Team is required to review and approve the classification of all data and information and determine the appropriate level of security and access that is best suited to protect such information.

User System and Network Access

7.7 The LLP's information technology users are all required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other staff member or third party whatsoever.

7.8 All users must comply with the following rules regarding the creation and maintenance of passwords:

(a) passwords must not be found in any English or foreign dictionary (i.e. they do not use any common name, noun, verb, adverb, or adjective as these can be

easily cracked using standard "hacker tools");

(b) passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal;

(c) user accounts at the LLP will be frozen after 5 failed logon attempts and require reenabling by the Systems Administrator;

(d) logon IDs and passwords will be suspended after 90 days without use; and

(e) passwords will be based on Windows 2012R2 Server standard complexity standards complexity standards.

7.9 Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this Policy.

7.10 Employee Logon IDs and passwords will be deactivated as soon as possible if the staff member's contract is terminated or they are fired, suspended, placed on leave, or otherwise leave the employment of Cibus.

7.11 Supervisors/Managers shall immediately and directly contact the Systems Administrator to report change in employee status that requires terminating or modifying employee logon access privileges.

7.12 LLP staff who forget their password must first contact Fred Appleby (07715316902) or secondly the IT department at Computer Care (02031009317) to get a new password assigned to their account. The LLP's members/partners and staff should always clearly identify themselves to the aforementioned IT professionals during any communication.

7.13 LLP members and staff will be responsible for all transactions that occur during logon sessions initiated by the use of such person's password and ID.

7.14 LLP members and staff shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

Special Access

7.15 Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job (such as contractors or summer interns etc).

7.16 These accounts are monitored by Cibus members/partners and require the permission of the user's Systems Administrator.

7.17 Monitoring of the special access accounts is done by entering the users into a specific area or folder. System Administrators or higher can generate reports that will show who currently has a special access account, for what folder or area and when it will expire. Special accounts will expire as required and will not be automatically renewed without written permission.

Third Party Access

7.18 "Third-party" refers to vendors, consultants and business partners doing business with Cibus, and other partners that have a need to exchange information with the LLP. Third-party network connections are to be used only by the employees of the third-party and only for the business purposes of the LLP.

7.19 The third-party company will ensure that only authorised users will be allowed to access information on the LLP's network.

7.20 The third-party will not allow internet traffic or another private network traffic to flow into the network.

7.21 This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

7.22 All requests for third-party connections must be made by submitting a written request and be approved by the IT Systems Administrator.

Connecting Devices to the Network

7.23 Only authorised devices may be connected to the LLP's networks. Authorised devices, including PCs and workstations owned by the LLP, must comply with the configuration guidelines of the LLP as prescribed by its Systems Administrator. Other authorised devices include network infrastructure devices used for network management and monitoring.

7.24 Non-LLP computers that are not authorised, owned and/or controlled by the LLP's Systems Administrator shall not attach to the network. All non-LLP owned devices must be approved by the LLP's IT Systems Administrator.

7.25 Users are not authorised to attach any device that would alter the topology characteristics of the LLP's network or any unauthorised storage devices, e.g., thumb drives and writable CDs.

Remote Access

7.26 Remote Access refers specifically to external users accessing the Cibus share platform, as opposed to LLP Members and staff working remotely. Only authorised and contracted external parties may remotely access the LLP's network. Remote access is provided to those members, employees, contractors and business partners of the LLPs that have a legitimate business need to exchange information, copy files or programs,

or access computer applications.

7.27 Authorised connections can be created via a secure link to a specific file or folder with no access to the wider SharePoint platform and only with express written permission from a senior Member of the LLP. The only acceptable method of remotely connecting into the internal network is using a secure ID.

Unauthorised Remote Access

7.28 The attachment of (e.g. hubs) to a user's PC or workstation that is connected to the company LAN is not allowed without the written permission of the Systems Administrator.

8. EMAIL AND DEVICES

Emails

8.1 The LLP's members and staff should use care when sending emails externally to ensure that they comply with acceptable standards in terms of content and that they do not contain confidential information that should remain for internal use only.

8.2 Emails sent to external parties containing links to OneDrive folders must have an expiration date set on the link and read only status enabled for the end user.

8.3 Emails sent from LLP user accounts are scanned using Office 365 content and compliance rules to help prevent confidential data leakage as well as for malware.

Portable Data Storage

8.4 All Cibus laptops have had the USB ports restricted to eliminate data transfer and prevent a data loss scenario should a laptop be lost. The LLP's members and staff must take special care of data stored on any form of portable storage such as USB Drives/Data Sticks. Ideally these should not be used but where necessary these should be encrypted. Such USB Drives/Data Sticks should be stored securely and employees must report to the Compliance Team immediately if any confidential information has been lost.

Laptops and Portable Devices

8.5 Laptops are protected with Trend anti-virus software and have an RMM Client installed to allow remote access by the IT consultants in the case that the hardware is misplaced [and needs to be wiped].

8.6 All LLP laptops are synchronised in real time with Microsoft OneDrive which is in turn backed up using Datto backup software which backs up the entire dataset three times daily. However, LLP members and staff should exercise care when handling laptops to ensure that they are not left in locations where others can access them and to report a loss immediately to the LLP's Compliance Team.

9. **TESTING**

9.1 The LLP's internal networks are protected by a Fortinet Firewall and Cyberoam with Firepower Services, offering comprehensive threat protection and intrusion detection. Cibus uses Codex Software Development Ltd to perform penetration testing on a monthly basis. From the 1st July 2025, the LLP transitioned to a fully managed service operated by Computer Care that employs Todyl software as well as a host of enhanced email security measures. The new contract will deploy monthly phishing tests to all staff.

10. **COMPLIANCE AND ENFORCEMENT**

Penalties for Violation

10.1 The LLP treats cyber security issues very seriously. Individuals who use the technology and information resources of the LLP must be aware that they can be disciplined and/or have their employment/membership terminated if they violate this Policy.

10.2 Upon violation of this policy, LLP members and staff may be subject to discipline up to and including discharge, suspension or reporting to the local police. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of this Policy, prior violations of this Policy by the individual and all other relevant information. Discipline which may be taken against LLP members and staff shall be administrated in accordance with the LLP's Compliance Manual and Staff Handbook.

10.3 In a case where this Policy is breached by a person who is not a member or staff of the LLP, the matter shall be submitted to the LLP's Compliance Team for appropriate action. The Compliance Team may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

Security Incident Handling Procedures

10.4 The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network. Some examples of security incidents are:

(a) illegal access of the LLP's computer system. For example, a hacker logs onto a production server and copies the password file;

(b) damage to an LLP computer system or network caused by illegal access. For example, releasing a virus or worm;

(c) denial of service attack against an LLP web server. For example, a hacker initiates a flood of packets against a web server designed to cause the system to crash; or

(d) malicious use of system resources to launch an attack against other computers outside of the LLP's network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

10.5 The LLP's members and staff who believe their hardware or computer systems have been subjected to a security incident, or have otherwise been improperly accessed or used, should report the situation to the LLP's Compliance Team immediately and notify the IT consultants Computer Care (support@computerc.co.uk) and James Buist (james.buist@cibuscap.com) or Fred Appleby (fred.appleby@cibuscap.com). The staff member should not turn off their computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

11. PORTFOLIO COMPANIES

11.1 The LLP is the investment adviser to several funds (together the **"Cibus Funds"**) and has regular communication with the portfolio companies of the Cibus Funds (the **"Portfolio Companies"**). Such communications will often include information that is confidential/sensitive in nature such as bank details, transaction information or personal data.

11.2 We expect all suppliers and partners with access to our data or systems to meet equivalent standards of security and data protection. Formal due diligence is conducted before engagement by the Technology Subcommittee, and contracts include clear clauses on data security, breach notification, and data transfer. International transfers are managed in accordance with UK GDPR, using Standard Contractual Clauses or appropriate safeguards.

11.3 It is noted that Portfolio Companies may not have the same standards of cyber security as the LLP (for example, they may use unsecured servers and non-encrypted messages). Accordingly, through communications with Portfolio Companies, the LLP exposes itself to cyber incidents such as scams and hacking attempts.

11.4 It is the responsibility of the relevant LLP members and staff (together the **"Deal Team"**) to ensure that a minimum standard of cyber security is in place for the Portfolio Companies with which they communicate. As an indicator, all majority owned Portfolio Companies should adhere to the equivalent of the UK's "Cyber Essentials" Certification at a minimum (noting that non-UK companies will not be able to obtain the certification, but should enact the same level of precautions as required by the certification). All Portfolio Companies should have comprehensive cyber insurance in place.

11.5 As at the date of this Policy, the LLP is undertaking a review of all Portfolio Companies cyber security procedures and insurance. This review has been outsourced to a specialist third party consultant who has undertaken to have their initial review completed by Q3 2025 with the implementation and roll out of security measures and insurance complete by December 2025.

11.6 When assessing a new potential Portfolio Company, the Deal Team should conduct cyber due diligence and this, together with cyber insurance, forms part of the "transaction checklist" which must be completed before any new Portfolio Company is acquired.