Cibus Capital LLP

Cyber Security Policy

LEGAL DISCLAIMER. PLEASE READ BEFORE CONTINUING:

This document is confidential, provided for informational purposes only and is not legally binding on Cibus Capital LLP ('Cibus') or any of its affiliates.

None of Cibus or any of its affiliates accept 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.

This document relates to Cibus Capital LLP's current operations as of 23 November 2022 but is liable to change at any time without notice.

Dated: 23 November 2022

OVERVIEW

This Cyber Security Policy is a formal set of rules by which Cibus Capital LLP's member/partners, staff and other persons who are given access to Cibus Capital LLP's technology and information assets must abide.

The Cyber Security Policy serves several purposes. The main purpose is to inform Cibus Capital LLP users, including members/partners, staff, consultants, contractors and other authorised users of their obligatory requirements for protecting the technology and information assets of Cibus. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

This Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of Cibus' computer systems and network.

WHAT WE ARE PROTECTING

It is the obligation of all users of Cibus' systems to protect the technology, information assets and confidential data of Cibus. This information must be protected from unauthorised access, theft and destruction. The technology and information assets of Cibus are made up of the following components:

- Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
- System Software including operating systems, database management systems and backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within Cibus. This includes custom written software applications and commercial off the shelf software packages.
- Communications Network: hardware and software including routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

Classification of Information and Appropriate Access

The default access level of all staff user profiles is, 'Basic User Level Access' meaning that they have access to common share files and nothing else. 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 Global Administrator Level Users. Global Administrators are James Buist, Cibus IT Consultant, Fred Appleby, the Cibus in house IT specialist and Computer Care, the third-party IT consultant.

The 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.

Chief Information Officer. Cibus shall appoint a Chief Information Officer of Data and Information Technology. The current Chief Information Officer is Mr James Buist.

Security Administrator. Cibus shall appoint a Security Administrator for administering its data and information security. The current Security Administrator is Mr James Buist.

Threats to Security

Employees
One of the biggest security threats is employees. They may do damage to Cibus' systems either through incompetence or with malicious intent. Cibus should layer its information technology security to compensate for employee threats. This includes the following procedures:

- Only give out appropriate rights to systems to appropriately senior staff.
- Do not share accounts to access systems. Cibus' members/partners, staff should *never* share login information with co-workers or third parties.
- When any Cibus staff contract is terminated, or the staff member is suspended or otherwise disciplined, Cibus should typically remove or limit access to systems and change passwords.
- Advanced – Cibus keeps detailed server access logs on computer activity.

Email Phishing
Phishing emails are more common now than ever and whilst the majority are filtered out through the spam filter built into Office 365 and Cibus' firewall, occasionally one will make it into a staff inbox. Cibus' staff are able to recognise a phishing or 'clickbait' email and are trained to be cautious when clicking on poorly explained links within emails ("Click here to win a prize/watch this video!"). **Employees 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
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. 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.
These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually 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.

Cibus maintains firewalls and password logins as a protection against this risk.

Criminal Hackers and Saboteurs.
The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

Whilst this is a remote threat for a business of the nature of Cibus, Cibus maintains firewalls and password logins as a protection against this risk.

USER RESPONSIBILITIES

This section establishes usage policy for Cibus' computer systems, networks and information resources. It pertains to all employees and contractors who use Cibus' computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for Cibus' business purposes.

Acceptable Use

User accounts on Cibus' computer systems are to be used only for business of the company and not to be used for personal activities. Unauthorised use of the system may be in violation of the law, constitutes theft and can be punishable termination of employment, suspension and/or may contravene applicable laws. Unauthorised use of the company computing system and facilities may constitute grounds for either civil or criminal prosecution.

Cibus'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, Cibus staff are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised persons outside Cibus and its affiliates.

Cibus users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources for their own use; or gain access to those parts of Cibus' systems for which they do not have authorisation.

Cibus users shall not 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.

Cibus users shall not download unauthorised software from the internet onto their PCs or workstations.

All Cibus members/partners and staff are required to report any weaknesses in the firm's computer security and any incidents of misuse or violation of this policy to their immediate supervisor and/or Cibus' Chief Information Officer or Systems Administrator.

Use of the Internet

Cibus will provide internet access to employees and contractors who are connected to the internal network. Employees and contractors should obtain wi-fi access codes from the Security Administrator.

The internet is a business tool for Cibus. 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.

The 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 Cibus' Employee Handbook.

User Responsibilities

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

User Category	Privileges & Responsibilities
Department Users (Cibus Members & Employees)	Access to application and databases as required for job function. (RED and/or GREEN cleared)
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.
Security Administrator	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
Systems Analyst/Programmer	Access to applications and databases as required for specific job function. Not authorised to access routers, firewalls, or other network devices.
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 Cibus Management Board. Access should be monitored and revoked on termination of the contractual relationship.
Other Agencies and Business Partners	Access allowed to selected data rooms, and log-in portals only in connection with their relationship with Cibus.
General Public	Access is limited to information on Cibus' public website. The general public will not be allowed to access confidential information.

Monitoring Use of Computer Systems

Cibus Capital LLP has the right and capability to monitor electronic information created and/or communicated by persons using Cibus' computer systems and networks, including e-mail messages and usage of the internet. Emails and documents created by Cibus' members/partners and staff in connection with their employment are the intellectual technology and property of Cibus. It is not Cibus' current policy to continuously monitor all computer usage by members/partners, staff or other users of Cibus' computer systems and network. However, users of the systems should be aware that Cibus 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 Cibus' internal policies.

ACCESS CONTROL

A fundamental component of Cibus' Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorised disclosure or modification.

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.

User System and Network Access – Normal User Identification

All Cibus information technology users will be 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. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools."
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password must be changed regularly – recommended every 90 to 180 days.
- User accounts at Cibus will be frozen after 5 failed logon attempts and require reenabling by the Systems Administrator.
- Logon IDs and passwords will be suspended after 90 days without use.
- Passwords will be based on Windows 2012R2 Server standard complexity standards.

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 Cyber Security Policy.

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.

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.

Cibus staff who forget their password must call the IT department to get a new password assigned to their account. Cibus members/partners and staff should always clearly identify themselves to the IT department during any communication.

Cibus members/partners and staff will be responsible for all transactions occurring during logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

System Administrator Access

System Administrators, network administrators, and security administrators will have System Administrators access to host systems, routers, hubs, and firewalls as required to fulfil the duties of their job.

All system administrator passwords will be deleted immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of Cibus.

Special Access
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). These accounts are monitored by Cibus members/partners and require the permission of the user's Systems Administrator. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire. Special accounts will expire in as required and will not be automatically renewed without written permission.

Third-Party Access to Cibus Network.
This policy is established to ensure a secure method of connectivity is provided between Cibus and all third-party companies and other entities required to electronically exchange information with Cibus.

"Third-party" refers to vendors, consultants and business partners doing business with Cibus, and other partners that have a need to exchange information with Cibus. Third-party network connections are to be used only by the employees of the third-party and only for the business purposes of Cibus. The third-party company will ensure that only authorised users will be allowed to access information on Cibus' network. The third-party will not allow internet traffic or another private network traffic to flow into the network.

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.

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

Non-Cibus computers that are not authorised, owned and/or controlled by Cibus' IT Systems Administrator shall not attach to the network. All non-Cibus owned devices must meet with Cibus' IT Systems Administrator's approval.

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

Remote Access
Only authorised persons may remotely access Cibus' network. Remote access is provided to those employees, contractors and business partners of Cibus that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorised connection can be remote PC to the network or a remote network to Cibus' network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

Unauthorised Remote Access
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 Cibus' IT Systems Administrator.

Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorised highly secure methods of remote access and poses a threat to the security of the entire network.

EMAIL

Cibus members/partners and staff should use care when sending emails 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. 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.

Emails are scanned using Office 365 content and compliance rules to help prevent confidential data leakage as well as for malware.

PORTABLE DATA STORAGE

Cibus Capital LLP members/partners 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. They should be stored securely and employees must report to the Compliance Team immediately if any confidential information has been lost.

LAPTOPS & PORTABLE DEVICES

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. All 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, Cibus 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 Cibus' Compliance Team.

INTRUSION DETECTION & TESTING

The Internal networks are protected by a Cisco 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.

PENALTY FOR SECURITY VIOLATION

Cibus treats Cyber Security issues very seriously. Those people who use the technology and information resources of Cibus must be aware that they can be disciplined and/or terminated if they violate this Cyber Security Policy. Upon violation of this policy, Cibus 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 the Cyber Security Policy, prior violations of the policy committed by the individual and all other relevant information. Discipline which may be taken against Cibus staff shall be administrated in accordance with Cibus' Compliance Manual and Employee Handbook.

In a case where this Cyber Security Policy is breached by a person who is not a member of Cibus staff, the matter shall be submitted to Cibus' Compliance department 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

This section provides some policy guidelines and procedures for handling security incidents. 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:

- Illegal access of Cibus' computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a company computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a Cibus web server. For example, a hacker initiates a flood of packets against a web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computers outside of Cibus' network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Cibus members/partners and staff who believe their terminal or computer systems have been subjected to a security incident, or have otherwise been improperly accessed or used, should report the situation to Cibus' Compliance department immediately and notify the IT consultants Computer Care (www.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.