CONFIDENTIALITY POLICY AND PROCEDURE

Revision Details

Issued by:	T. Lombard
Revised by:	T. Lombard
Approved by:	W. Steyn
Revision notes:	Annual review and document register/reference update

1 POLICY

CoZero shall, through legally enforceable commitments, implement a policy of the confidentiality of the information obtained or created during validation or verification activities. All employees, committees, external consultants, contractors, personnel of external bodies or individuals acting on behalf of CoZero will be bound by this policy.

Information about a client shall not be disclosed to a third party without the written consent of the client, and when a disclosure is required by law, the client will be notified in writing in advance of the information being disclosed. Information about the client from an outside source, such as a complainant or regulators, will be treated as confidential.

CoZero shall use facilities and methods that will ensure secure handling of confidential information.

2 PROCEDURE

2.1 Legally Enforceable Commitments

- CoZero's letter of appointment includes a clause which binds all employees to the confidentiality requirements in regard to client and company information as described in the company's policy on confidentiality. All employees are required to sign the letter of appointment upon commencing employment.
- All CoZero employees shall sign the Annual Compliance Declaration (00CZ00-MF-0010), stating their compliance with all CoZero's policies and procedures, including confidentiality.
- The verification service agreement (ref. 00CZ00-MA-0001) shall be signed by the verification team and the client at the kick-off meeting. This outlines the confidentiality requirements of the client and CoZero.
- Where very sensitive information may be disclosed to CoZero an additional non-disclosure agreement may be signed with the client.
- In instances when CoZero has to make use of consultants or experts, the terms or reference, including confidentiality issues, will be included in the letter of appointment. Consent from the client will be obtained in the case where a consultant will be appointment to perform duties on behalf of CoZero.

2.2 Client Information Disclosure

- If the information is to be placed in the public domain, or made available to a third party, such as to the DTI or SANAS, CoZero shall obtain their consent thereto.
- If a third party requests information pertaining to CoZero's client, such as their emission levels and types, or any aspect pertaining to the results of the verification process, that party will be referred back to the client, and the client should request in writing that CoZero make the information available to the third party. The analyst (receiver of the request) will forward it to the Verification Committee, which will give consent to release the information. Only then can the information be revealed to the third party and the approval by the client will be filed in the client file.
- Information that is not public information will not be disclosed to a third party.

2.3 Confidentiality of Client Files

- All completed project files will be scanned and saved on CoZero's server before file sign-off and hard copies of files are destroyed after a minimum of 5 years. Backups are kept off-site and backed up daily, so as to ensure that the client's information is secure. In accordance with CoZero's Control of Records Policy (00CZ00-MP-0003), all hard copy client files will be scanned onto the network server.
- The confidentiality issues relating to the control of records is further detailed in the Control of Records Policy and procedure.

2.4 Equipment, Facilities and Information Technology to ensure confidential handling of information

Use of Laptops

Laptop computers taken outside of the CoZero environment are subject to special security risks: they may be lost or stolen and may be exposed to unauthorised access or tampering.

Laptop loss will mean not only the loss of availability of the device and its data, but may also lead to the disclosure of sensitive information. This loss of confidentiality, and potentially its integrity, will often be considered more serious than the loss of the physical asset.

Where large quantities of CoZero data are held on a single laptop (or any other storage medium) risk assessments must consider the impacts of loss of all the data. Note that deleted files should be assumed to persist on the laptop's hard disk.

Personnel will log into the CoZero server or via Dropbox which is secured to work remotely on their laptops.

Tampering of CoZero Computers/Laptops

Each laptop/computer has been specifically configured for that employee to meet their daily duties. Under no circumstance is any employee authorized to alter or amend, add or delete any programs, without the authorization of the IT administrator.
All inappropriate misuse to the system and its programs will be recorded on all events and referred to the appropriate managers for disciplinary action to be taken if necessary.

❑ Access Control and Password Control

Access to information must be granted based on an individual's job responsibilities and/or a valid need-to-know basis. Unauthorized access or use of an individual's account is prohibited.

All employees shall be issued with a password. Passwords should be controlled in accordance to the following guidelines:

- The Password shall consist of alpha and numerical characters in both upper and lower case.
- Passwords should not be "guessable".
- Passwords should be considered personal and must be well protected.
- Passwords must not be written down and left in a place where unauthorized persons might discover them.
- Passwords should not be sent through internet e-mail unless securely encrypted.
- Passwords must not be disclosed or shared with anyone.

Upon leaving a workstation employees shall lock their password protected screensaver or log off.
Employees shall:

- Ensure that all computers are logged off and switched off upon leaving the office.
- The office is locked when leaving the laptop unit unattended.
- When travelling and not in use, ensure that laptops are stored securely out of sight. Laptops left on display and unattended will inevitably attract attention and are likely to be stolen.
- The server shall be safeguarded as far as possible.

❑ Backup and disaster recovery

All employee work shall be done on the network and where any work is done off site such work shall be saved on the network as soon as the employee is back in the office.

Backup shall be done daily.

❑ Company proprietary information and confidentiality

All intellectual property and information written, generated and produced by any employee whilst in the employ of CoZero is the property of the company and may not be used for any other purpose.

CoZero reserves the right to access the contents of any messages sent over its facilities if the company believes, in its sole judgement, that it has a business need to do so. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Employees shall ensure that all data is removed from a disk/ USB storage disk when transferring data from clients. In particular, no other client data shall be made visible to a client when data is being transferred by USB storage disk.

❑ Use of e-mail and internet

Acceptable Usage:
The e-mail and internet facilities are company property and are to be used for business purposes. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Employees may:

- Use the Internet to obtain business information from reputable Internet sites.
- Access databases for information as needed.
- Use e-mail for business contacts.
- Use the facilities for appropriate and personal use such as internet banking and bookings, this can ensure that employees are not inconvenienced during working hours.

Unacceptable Usage:
Employees must not use the Internet for purposes that are illegal, unethical, harmful to the company, or nonproductive. The below are examples of unacceptable email/internet usage:

- Employees shall not access pornographic or untasteful media and transmit any content that is offensive, harassing or fraudulent.
- Employees shall not connect to any other network whilst connected to that of CoZero.
- Employees shall not send or forward chain e-mail, i.e., messages containing instructions to forward the message to others.
- Conduct a personal business using company resources.
- Employees may not use company facilities for any commercial or personal advertisements, solicitations or promotions of any outside business, political lobbying or promoting political activities.
- Employees may not download any media files (videos/movies and torrents) using CoZero's internet facilities.
- An employee who uses any company resource for illegal activity could be subject to summary dismissal conditional, on the effecting of the Disciplinary Code and Procedure.

All employees should note that all e-mail and logs of websites accessed are visible to the IT administrator and that personal usage of CoZero's email and internet facilities shall not be considered private.

❑ Communications channels

Wi-fi, Infrared and Bluetooth interfaces should be disabled by default or their switches set to the 'off' position. If wireless communication is permitted the laptop should be secured by following the good practice guidelines.

❑ Computer Scheme

Computers and related equipment are issued to employees but remain the property of CoZero. The value of the computer is amortized over a 3 year period. CoZero will insure the laptop provided to you.

You will be required to pay the Excess amount of R500 (as amended from time to time in accordance to Insurance rates). Should the Insurance not pay out for a stolen/lost laptop due to whatsoever reason you will be held liable for the replacement value of the laptop. You will also be held liable for the replacement value of the other items listed in S2505_IT Hardware Acceptance Form due to any loss, theft or damages to these items.

CoZero expects that Laptops and other company provided assets shall be safeguarded at all times, shall not be visible in vehicles or left overnight in vehicles and should not be left unattended at clients or anywhere where the laptop/other assets are at risk.

In the event of theft or loss and in order to protect the intellectual property of CoZero and with specific reference to BEESmart, the employee will be required to sign an affidavit confirming the theft or loss and that they do not have any copies of any CoZero proprietary programmes, files, confidential information, any client details or account details (including value fees), or any CoZero intellectual capital on another computer.

Should an employee leave before the 36 month period has passed, CoZero will assess the condition of the computer in conjunction with their IT service provider and determine the value of the computer and book value respectively. Where the computer has a value of less than the book value as a result of abuse thereof, CoZero may recover the deficit from the employee's last salary payment.

❑ CoZero Information Security Principles and Policy:

○ Security of equipment off-premises

- Security should be applied to off-site equipment taking into account the different risks of working outside the organisation's premises;
- Regardless of ownership, the use of any information processing equipment outside the organisation's premises should be authorised by management;
- Security risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

○ Baseline Information Security Standards.

❑ General Management:

- The Financial Manager shall take overall responsibility for the management of each CoZero organisation's laptop estate.

❑ Registration:

- All laptops used for CoZero business should be uniquely identified and registered in the organisation's records as information governance security-relevant items.

❑ Accountability:

- Responsibility for the security of an CoZero organisation's registered laptops and their data should be assigned to individuals and tracked alongside the employment status of those individuals.

Management of laptop security functionality:

- The installation and configuration of laptop security functionality, including access control, encryption and tamper resistance should be undertaken by appropriately trained staff.

○ Authorisation:

Regardless of a laptop's ownership, the use of any equipment outside an CoZero organisation's business premises for the processing of CoZero information must be authorised by the relevant Director or relevant Manager.

○ Physical:

- It is recommended that laptops, even when protected by disk encryption, should not be left in the care of any person who is not trusted to protect the information it contains.

○ Remote Access:

- Remote access from a laptop to CoZero information systems must be achieved via the selected VPN username and password that has been set up by the IT Administrator.

○ Data Storage and use:

- Sensitive data, stored on an CoZero laptop should be kept to the minimum required for its effective business use in order to minimise the risks and impacts should a breach occur.

○ Incident Reporting:

- Loss of CoZero laptops should be reported to the direct Manager as well as the Financial Manager.
- IT related incidents shall be reported to the Financial Manager and the IT Administrator.

○ Other good practice security measures

- Do not leave laptops unattended in car boots overnight.
- Do not leave laptops unattended in insecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available.
- Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc and on public transport e.g. buses and trains.
- Do not use laptops with removable media in places where that media could easily left behind or misplaced.
- When travelling, avoid placing laptops in locations where they could be easily forgotten or left behind e.g. Overhead racks and taxi boots.