Cybercrime Warning and Disclosure

For Cultivating Carbon (Pty) Ltd

1. What is cybercrime?

In general, cybercrime is a criminal activity that involves the use of computers, networks and the internet to commit illegal activities such as identity theft, hacking, phishing, malware and other forms of cybercrime. The Cybercrimes Act, 19 of 2020 provides a detailed description of what is considered a cybercrime in South Africa.

Cybercrime is a growing problem, with new threats and techniques emerging all the time. Cybercrime can include, but is not limited to, the following types:

1. Cyberterrorism
2. Identity Theft
3. Cyberstalking
4. Phishing
5. Malware
6. Hacking
7. Cyberbullying
8. Data Breaches
9. Botnets
10. Social Engineering
11. Denial of Service (DoS) Attacks
12. Fraud and Financial Crimes
13. Spam
14. Online Harassment
15. Intellectual Property Theft
16. Salami Attacks
17. Cryptojacking
18. Website Defacement
19. Scams
20. Software Piracy.

2. Techniques to protect yourself.

- **Install anti-virus and malware protection and keep it up to date**: Install a reputable anti-virus and malware protection program on all of your devices. Make sure your protection is always updated to the latest version.

- **Use strong passwords**: Create strong passwords that are difficult to guess and use different passwords for each of your accounts.

- **Be wary of links in emails and on websites**: Be cautious when clicking links in emails or on websites. Cyber criminals often use malicious links to gain access to your computer or personal information.

- **Use two-factor authentication**: Two-factor authentication is a great way to add an extra layer of security to your accounts. It requires you to enter a code sent to your phone or email, in addition to your password, to access the account.

- **Regularly back up your data**: Regularly back up your data and save it to an external hard drive or cloud storage service, such as Dropbox or Google Drive. This way, if your computer is compromised, your data will be safe and secure.

- **Use a VPN**: If you're using public Wi-Fi, use a virtual private network (VPN) to secure your internet connection.

3. Business email compromise (BEC)

BEC is a specific form of a phishing scam that targets organisations to either steal money or valuable information. Employees receive emails from what appear to be a trusted source. Attackers can impersonate users or domains making small almost unnoticeable changes to email addresses. It is important to note that either the client's or the organisation's emails can be compromised. Once a user's trust has been gained, the attacker can provide fake invoices or amend bank account details to make a transfer to the attacker's account. Cultivating Carbon has put in place all appropriate, reasonable technical and organisational security measures to protect the integrity and confidentiality of our client's information and our systems. It remains important though that our clients and other third parties also take steps to verify bank account details before making payments to anyone by, for example, phoning a known employee and verifying that the account details you have is correct.

Cultivating Carbon only conducts its services with clients through formal processes and agreed upon communication channels. Be aware that individuals may fraudulently attempt to solicit business by impersonating or claiming to be a representative of Cultivating Carbon using messaging services or other social media platforms. Cultivating Carbon will never inform you of changes to our banking details by way of an *ad hoc* email. Please inform us immediately should you receive such an email.