CYBER SECURITY POLICY

1. INTRODUCTION

1.1 This cyber security policy ("**Policy**") outlines the processes and procedures governing the selection and use of Information Technology/IT (*defined below*) resources of TruAlt Bioenergy Limited ("**Company**"). The Company's IT assets shall be used responsibly by all the Users (*defined below*) in accordance with the scope and extent of their respective roles and responsibilities with the Company, and only for the purposes of discharging their duties and obligations towards the Company.

1.2 The various IT assets are made available by the Company to the Users to allow the Users to access the IT systems and resources in order to effectively execute their roles, responsibilities, functions and duties towards the Company and its business and operations. The usage of the Company's IT assets made available to the Users is, in addition to this Policy, also subject to various other policies of the Company on the respective subject matter, as may be introduced, amended or revised from time to time, at the sole discretion of the Company.

2. PURPOSE

2.1 This Policy is applicable to all the IT resources and assets of the Company, whether software or hardware, including computer systems, email accounts, applications, databases, storage devices, network systems, network devices and security monitoring systems, including any component thereof which form a part of the business and operational processes of the Company.

2.2 This Policy will be applicable to all the Users using any IT asset of the Company, whether directly or indirectly, irrespective of whether working within or outside the Company's office premises. This Policy is also applicable to the IT administered centrally, on personally owned computing devices by wire/wireless to the Company's IT network and to off-site computing devices that connect remotely to the Company's IT network.

3. SCOPE

3.1 The Company is committed to practice and carry on its business and operations in a secure and private manner. In light of the various information technology laws, including recent legislations in respect of data privacy laws, the Company is driven to formulate and maintain a secure cyber network for all the Users and the Company, and to further ensure that the Company's Confidential Data (*defined below*) is well managed and protected.

3.2 This Policy is effective from 22nd July 2024 and will supersede all prior policies, notices and communication in connection with the subject matter. This Policy will be posted on the Company's website at https://www.trualtbioenergy.com/

4. DEFINITIONS

4.1 **"Confidential Data"** means and includes, without limitation, the following information in respect of the Company and its subsidiaries/affiliates:

(a) Unreleased and classified financial information, budgets and other financial details;

(b) Customer, supplier, vendor, contractor, employees, consultants, agents, partners, affiliates and shareholders information;

(c) Proprietary information relating to development, marketing, customer leads, sales-related data, operation and performance;
(d) Computer programs, source code, technical drawings, algorithms, know-how, formulas, processes, ideas, inventions (whether patentable or not), schematics and other technical, business, financial, customer and product development plans, forecasts, strategies and information;
(e) Patents, business processes, proposed businesses, specifications, research, trade secrets and/or new technologies;
(f) Sensitive Personal Data (*defined below*);
(g) Computer programming techniques, methodologies and related technical information, operating manuals, equipment, software, designs, technology and technical documentation;
(h) Users' passwords, assignments, and personal information; and
(i) Company's contracts and legal records.

4.2 **"Cyber Security"** means a body of technologies, processes and practices designed to protect networks, computers, programs, data and personal information, including the Confidential Data and IT of the Company from attack, damage or Unauthorized Access *(defined below)*;

4.3 **"Information Technology"** or **"IT"** means and include all software, hardware, firmware, telecommunications systems, network systems, embedded systems and other systems, components and/or services that are owned or used by the Company and/or its subsidiaries/affiliates in the conduct of its/their business and/or operations;

4.4 **"Relevant Laws"** means the data security and data privacy laws of India, which includes, without limitation, the Information Technology Act, 2000, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**IT Rules**"), the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 and the Digital Personal Data Protection Act, 2023 (which shall be applicable once the same is made effective by way of a notification by the Government);

4.5 **"Sensitive Personal Data"**, in accordance with the IT Rules, means such personal data which consists of information relating to:

(a) Passwords;
(b) Financial information such as bank account or credit card or debit card or other payment instrument details;
(c) Physical, physiological and mental health condition;
(d) Sexual orientation;
(e) Medical records and history;
(f) Biometric information;
(g) Any other details relating to the above mentioned, provided by any person to the Company for providing services; and
(h) Any information received pursuant to the above by the Company for processing or storing such information under a lawful contract or otherwise,

Provided that any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force will not be considered to be Sensitive Personal Data;

4.6 **"Unauthorized Access"** means any access of any kind, whether digitally or physically, by a person to an electronic system or data held in an electronic system which is ***(a)*** unauthorized or done without authority, ***(b)*** in excess of authority granted to such person, ***(c)*** without obtaining permission/consent to such access from a person/entity so entitled, and/or ***(d)*** without a business need or other lawful reason; and

4.7 **"Users"** mean and include all the employees, contractors, consultants, vendors, customers, shareholders, agents, representatives and other stakeholders of the Company (including its subsidiaries/affiliates) who access or receive information produced, stored or communicated by Company's IT systems, including the individuals who have the possession of Company's IT resources and assets and the individuals who connect with the IT network of the Company (including its subsidiaries/affiliates), whether directly or indirectly. Users also include all individuals, who by nature of their relationship with the Company (including its subsidiaries/affiliates) are entrusted with sensitive or Confidential Data of the Company (including its subsidiaries/affiliates).

5. PROCEDURES AND CONTROLS

5.1 Roles & Responsibilities

(a) **Senior Management**: The senior management includes individuals who hold the decision-making authority in respect of day-to-day management and operations of the Company, and they are responsible for endorsing and supporting Cyber Security initiatives, allocating resources and reviewing the effectiveness of the Cyber Security program/framework;
(b) **IT Department**: The IT department of the Company ("**IT Department**") is responsible for implementing the technical controls and the Cyber Security framework over the IT assets and resources of the Company (including its subsidiaries/affiliates), and to monitor the network infrastructure and respond to Cyber Security incidents, if any;
(c) **Users**: The Users are responsible for familiarizing themselves with this Policy, adhere to the guidelines and terms stated herein, participate in the training sessions and workshops as may be conducted by the IT Department in relation to this Policy and to immediately report any suspicious activities or Cyber Security incidents to the IT Department/immediate supervisor or manager.

5.2 Access Controls

(a) The Users shall be granted the access to the IT resources of the Company and the systems and related data shall be granted to the Users based on the principle of least privilege; and
(b) The Users shall follow and apply the authentication mechanisms, as may be prescribed by the IT Department, such as multi-factor authentication and such authentication mechanism shall be employed to access, amongst others, designated critical systems.

5.3 Data Protection

(a) Encryption shall be used to protect sensitive data (including Confidential Data), both in transit and at rest; and
(b) Regular data backups of the IT systems shall be performed, and such backups shall be stored in a secured manner to ensure data integrity and availability.

5.4 Awareness & Training

(a) Regular training sessions and workshops shall be conducted to educate Users in relation to the Cyber Security threats and subsequently, how to efficiently avoid such threats by way of safe computing practices; and

(b) Regular awareness programs to keep the Users updated in relation to various Cyber Security threats and methodologies employed by the scammers/hackers and to educate the Users about their significant role in maintaining the Cyber Security of themselves and the Company.

5.5 Computer, Email & Internet Usage

The Users are expected to use the internet responsibly in order to protect themselves and the Company. Inappropriate and/or unregulated use of the internet exposes the Company to multiple risks such as virus attacks, compromise of Cyber Security framework, IT assets and services, legal issues, etc. The acceptable usage of the internet, computer systems and email on the Company's IT systems shall be as stated below:

(a) Access to the internet shall only be exercised for official/work related activities and the Users shall not use the internet for personal purposes. Work related activities include research and educational data/information that may be found *via* the internet that would assist the User in carrying out his/her roles and responsibilities towards the Company (including its subsidiaries/affiliates);

(b) All data including Confidential Data that is composed, transmitted and/or received by Company's IT systems through the internet is considered to belong to the Company or its subsidiaries/affiliates, as applicable and is recognized as part of its/their official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties. The Users shall not use the internet, email, official handheld devices and/or computers to share the aforesaid data in any manner whatsoever, to any third party except as may be prescribed by the Company;

(c) The IT assets and services used to access the internet are the property of the Company and the Company reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections. Therefore, Users must take cognizance of their usage of the internet and to limit such usage strictly to carry out their roles and responsibilities towards the Company (and/or its subsidiaries/affiliates, as applicable);

(d) E-mails sent *via* the Company's email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar, obscene or harassing language/images;

(e) All websites and downloads may be monitored and/or blocked by the Company's IT Department if they are deemed to be harmful and/or not productive to business and operations of the Company (including its subsidiaries/affiliates); and

(f) The installation of software such as instant messaging technology and/or any other form of social media on the Company's IT System is strictly prohibited.

5.6 Unacceptable Usage (*without limitation*)

(a) Sending or posting discriminatory, harassing, threatening messages or images on the internet or *via* Company's email ID as may be provided to the Users;

(b) Using the Company's IT resources and assets to perpetrate any form of fraud, and/or software, film/video or music piracy;
(c) Stealing, using or disclosing other User's password without authorization;
(d) Downloading, copying or pirating software and electronic files that are copyrighted or without authorization;
(e) Disclosing Confidential Data of the Company outside of the Company;
(f) Hacking into unauthorized websites using Company's IT systems;
(g) Sending or posting information that is defamatory to the Company, its officers, directors, employees, consultants, shareholders, agents, representative, its products/services and/or customers;
(h) Introducing malicious software onto the Company's IT network and/or jeopardizing the Cyber Security of the Company's electronic communication systems, etc;
(i) Sending or posting chain letters, solicitations or advertisements not related to business purposes or activities; and
(j) Passing off personal views online as representing those of the Company.

If the Users are unsure about what constitutes as acceptable/unacceptable internet usage, then such Users shall confer with their supervisor regarding such actions, and take actions as instructed by their supervisor.

5.7 Device Control

(a) Users shall keep all Company-issued IT assets and resources such as tablets, computers, laptops and other mobile devices password-protected (minimum of 8 characters, which shall include at least an uppercase character, a lowercase character, a special character, a number and shall not include the User's names, the Company's name or any other personally identifiable information to ensure a reasonable degree of protection from Unauthorized Access);
(b) Users shall secure all relevant devices before leaving their desk to safeguard the Confidential Data;
(c) Users shall obtain authorization from the office manager and/or inventory manager before removing IT devices from the Company premises;
(d) Users shall refrain from sharing private passwords with co-workers, personal acquaintances and other Users;
(e) Users shall regularly update IT devices with the latest security software to maintain the Cyber Security standards and to mitigate the possibility of Unauthorized Access;
(f) If the Users are using their personal devices to carry out the roles and responsibilities towards the Company, such Users shall report this information to their respective management for record-keeping purposes. Further, the Users shall keep all such personal devices password-protected (minimum of 8 characters, which shall include at least an uppercase character, a lowercase character, a special character, a number and shall not include employees' names, the Company's name or any other personally identifiable information to ensure a reasonable degree of protection from Unauthorized Access);
(g) Users shall ensure installation of full-featured antivirus software on their devices to maintain the Cyber Security standards. Further, Users shall regularly upgrade anti-virus software on their IT devices to mitigate the possibility of Unauthorized Access;
(h) Users shall always use secure and private networks while using Company's IT systems and devices.

5.8 Email Control

Users must take note that protection of the email systems is a high priority as emails can lead to theft of Confidential Data, Unauthorized Access including, without limitation, scams and can carry malicious software/viruses such as worms, trojans and bugs. Therefore, Company mandates all the Users to:

(a) Verify the legitimacy of each email received, including the email address, the domain name, attachments, if any, and the sender's name;
(b) Any bank account to which payment(s) are to be made by the Company (including its subsidiaries/affiliates) must be appropriately verified as to its authenticity, including by way of confirmation over email and phone. Further, where there is a request for changing the aforesaid bank account(s), the authenticity of such bank account(s) are to be verified, including by way of confirmation over email and phone;
(c) Avoid opening suspicious emails and attachments, and clicking on links therein;
(d) Look for any grammatical errors or differences in the email address;
(e) Avoid clickbait titles and links; and
(f) Contact the IT Department of the Company regarding any suspicious emails.

5.9 Transfer Control

The Company takes cognizance of the security risks that are involved during the transfer of data, including the transfer of Confidential Data, internally or externally. To minimize such security risks, the Company mandates all the Users to:

(a) Refrain from transferring Confidential Data, including classified information, to outside/third parties except where authorised;
(b) Only transfer Company's data over Company networks or through emails or via authorised cloud systems/servers only;
(c) Obtain the necessary authorization from senior management prior to transferring of Confidential Data;
(d) Verify the recipient of the information and ensure they have the appropriate security measures in place;
(e) Adhere to Company's data protection procedures and confidentiality agreement to maintain Cyber Security and prevent Unauthorized Access; and
(f) Immediately alert the IT department of any breaches, malicious software and/or scams.

6. VIOLATION & CONSEQUENCES

Any violation of the provisions set forth under the Relevant Laws, including any other applicable laws, or a violation of this Policy by any User shall amount to gross misconduct and contravention, and shall likely lead to disciplinary action, which could include termination of employment/engagement of such User. Company's disciplinary protocols are based on the severity of violation. Unintentional violations may warrant a verbal warning, however, recurring violations of the equivalent nature may lead to a written warning, and intentional violations may lead to suspension and/or termination of employment/engagement, subject to the facts and circumstances of such violations.

7. COMPLIANCE

The Users shall comply with this Policy, including the Relevant Laws and other applicable laws of India. The Company shall also take steps to ensure compliance with the Relevant Laws, regulations and industry norms.

8. POLICY REVIEW & UPDATE

8.1 This Policy will be reviewed annually or as needed to ensure its effectiveness towards the maintenance of Cyber Security standards and relevance in addressing emerging cyber threats and technological advancements.

8.2 Adherence to this Policy is essential to safeguarding Company's IT assets and resources, including the Confidential Data, and maintaining the trust of our customers, partners, and stakeholders. All Users are expected to contribute to a secure cyber environment by understanding and following the guidelines outlined herein.
pany.