THE UNION SUGAR ESTATES COMPANY LIMITED

INFORMATION TECHNOLOGY AND INFORMATION SECURITY

1. Foreword

This document provides an overview of the security-related technologies and security measures that are in place at The Union Sugar Estates Company Limited ('USE' or the 'Company') to secure its IT assets (data, network, server infrastructure and endpoints).

The procedure may be referred to as 'the document' and Information Technology (IT) may be referred to as 'systems', 'information systems' or 'services' in the remainder of this document.

2. Context

Companies have been relying on information technology to conduct their business operations. The advent of the Internet as a communication medium with the external world has become essential yet it has opened new opportunities for cybercriminals.

Indeed, companies are increasingly being the target of cybercriminals whose actions can lead to loss of business and reputational damage particularly if adequate security measures are not in place.

This situation has prompted companies to address risks related to cyber threats and security breaches. USE has always adopted a prudent approach in terms of cyber security. Numerous technologies and measures have been implemented to protect the Company from cyber threats.

The purpose of this document is twofold. Firstly, it describes the current cyber threat landscape in which businesses are evolving. Secondly, it provides an overview of the security measures and technologies that have been implemented at USE to protect its IT assets.

Please note that this document does not supersede any existing or future policies, manuals, code of ethics, code of conduct, procedures or other agreements that the Company may define as it sees fit.

3. Roles and responsibilities

Cybersecurity is a company-wide concern. It begins with end-users and extends to the board room. It is important that all stakeholders understand the risks associated with cyber threats and be aware of the common threat vectors.

It has been recognised that adopting the right behavior in the business environment is a first and major step towards mitigating cyber-related risks.

4. Threat vectors

This is a list of threat vectors for which actions have been taken to prevent or mitigate cyber related risks:

- Malicious files and applications such as virus and malware. (Web-browsing, E-mail, Software, Download);
- Scams, phishing and spoofing of user identity (E-mail);
- Vulnerability exploit (O/S, Web-browsing, E-mail);
- Unauthorised access rights and privileges (Access control); and
- Denial of Service (Network attacks at the Internet gateway).

5. Overview of security measures

USE has adopted a prudent approach in respect to cyber security and has implemented practices with the objective to safeguard the IT assets. The main measures are described below:

- Secured physical infrastructure;
- IP addresses are assigned by the IT function, thus allowing end-users' identification;
- Controlled applications. End-users cannot install software or applications on their workstations and/or laptops. All applications are controlled and installed by authorised IT staff. This also ensures legal usage of software packages;
- Centralised update servers to download and deploy latest security patches and updates to all end-points; and
- Physically segregated and controlled Wi-Fi network to avoid potential data leakage and theft.

6. Technologies implemented

USE has deployed a number of technologies to protect its network infrastructure and mitigate cyber-related risks. The main technologies are described below:

➢ Centralised antivirus with administration platform, which allows:

- Automated download of latest virus signatures and antivirus engines;
- Automated deployment of virus signature databases to each end-point;
- Incoming emails controlled by anti-virus at the gateway;
- Scheduled scanning of all end-points;
- Online scanning when application is launched on end-points; and
- Monitoring of virus and malware identification on network.

➢ Administrator privilege on each end-point, which allows:

- Control of applications and software packages installed on workstations/laptops;
- Ensure compliance to end-user software agreement; and
- Genuine software installation and licenses control.

- Centralised patching and updates deployment, which allows:
  - Automated download of latest patches and updates for end-points;
  - Automated deployment of approved patches and updates to all end-points; and
  - Fast deployment of patches to all end-points.

- Wi-Fi access points for end-user and guest users, which are:
  - Password protected;
  - Physically isolated to the enterprise network;
  - IP addressing is independently handled by the Wi-Fi Access Point; and
  - Internet access is controlled and filtered by firewall.

- Awareness about latest cybersecurity threats and risks, through:
  - Communication by email to end-users about virus and malware outbreaks;
  - Communication by email to end-users about scam and phishing attempts; and
  - Behaviours to adopt when there is a scam or social engineering attempt.

- A defined backup and disaster recovery policy, which allows:
  - Full recovery of an impacted system in case of cyber-related issues;
  - Granular recovery of centralised backup data (e.g. specific files); and
  - Retention of data allowing specific recovery dates within the retention period.

Date: 27th March 2023.

H Charun