INFORMATION TECHNOLOGY & DATA MANAGEMENT SYSTEMS POLICY

PURPOSE AND SCOPE

As a developer of world's best practice geological repository waste solutions, Tellus Holdings Ltd and its related bodies corporate (together, "Tellus" or the "Company") are committed to promoting and maintaining a high standard of integrity, ethics, compliance, investor confidence and good corporate governance.

Tellus recognises the need to protect confidential and/or sensitive information stored or transmitted electronically and to ensure the protection of Tellus information technology resources. This Policy applies to anyone who is employed by or works at or for Tellus, including employees (whether permanent, fixed term or temporary), contractors, consultants, secondees and directors (collectively referred to as "Employees" in this Policy).

This Information Technology and Data Management Systems Policy (the "Policy") assigns responsibility and provides guidelines to protect Tellus systems and data against misuse and/or loss.

This Policy applies to the activities of Tellus, and the people associated with the Company. This includes staff, visitors, consultants, contractors, clients and key stakeholders. Tellus shall ensure that this Policy is communicated and understood throughout the Company and is available for access to relevant interested parties, as appropriate.

POLICY STATEMENT

Security

Multi Factor Authentication

All Tellus MSO365 Azure AD accounts will require fully enabled Microsoft Azure Multi-Factor Authentication (MFA) as an additional security measure to further verify user identity. MFA will be set up on all accounts using the Microsoft Authenticator App.

Conditional Access Policies

The Tellus Azure environment is configured with conditional access policies to severely reduce the potential for unauthorised user account access. These include:

- Enable MFA for all users
- Geo-blocking access outside of Australia. This requires users to lodge an exclusion when travelling internationally if system access is required, and
- Bypass MFA prompts for trusted locations as agreed with Tellus (e.g. offices and site locations)

Passwords

Each employee will set their own password for access to IT systems and will be required to follow the instructions below to ensure security levels are maintained:

- Passwords should not be easily guessable. Birthdays, Pet's name, etc. should be avoided
- You may be prompted to change your password from time to time and can also do so at any time if it determined it may have been compromised
- Passwords should never be written down and left in accessible/visible areas
- The sharing and communication of passwords is prohibited as this violates the security and integrity of files stored on PCs and systems that have been granted authorised access
- Logon ID and passwords should not be divulged over the phone or email. (This is not applicable to the Tellus IT and Communications Coordinator who may be required to email through logon information), and
- Your laptop must be locked when you are away from it to ensure no-one else can access it

Virus Protection

All devices must have supported anti-virus software installed and scheduled to run at regular intervals.

Users should also be aware of the following:

- External storage media like USB pen drives must be new or from a trusted source. Any external storage from an unknown source is not to be used
- Email attachments, especially those received from external sources, should be opened with caution
- Downloads should be limited to trusted and authorized sources only, and
- No software, shareware or freeware may be installed on any computer without approval of the Tellus IT and Communications Coordinator and must only be installed by Tellus IT Provider

Internet and Email

Tellus operates an MS Office 365 suite of software for electronic mail, sharing knowledge and project management. These systems are to be primarily used for conducting the Company's business and all messages composed, sent, received and stored on these systems remain the property of Tellus.

All sites and downloads may be monitored and/or blocked by Tellus if they are deemed to be harmful and/or not productive to business or are believed to cause a threat to the integrity of Tellus' IT system.

Unacceptable use of internet and email by employees includes, but is not limited to:

- Access to sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal material or any other site Tellus might consider inappropriate
- Access to gaming or gambling sites
- Sending or posting discriminatory, harassing, or threatening messages or images via Tellus' email service
- Sharing confidential material, trade secrets, or proprietary information outside of the organisation
- Sending or posting information that is defamatory to Tellus, its products/services, colleagues and/or customers
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities, and
- Passing off personal views as representing those of the organisation

Social Media

All employees must be mindful of how they represent themselves on social networks as the lines between public and private, personal and professional are becoming increasingly blurred. If they identify themselves as working for Tellus in a social network, they must ensure that content associated with them as an identifiable Tellus employee is consistent with their role in the organisation and doesn't compromise Tellus' brand and reputation.

Employees should refrain from posting any photos or comments that relate to Tellus company, project or other employees, contractors or suppliers, unless specifically asked to do so as a part of a Tellus marketing campaign. This includes images of work meetings, social events or other functions where you are representing the company.

Sharing of any company information that has been identified as 'not for public announcement' or otherwise embargoed is strictly forbidden. If you are unsure of whether any content or comment is suitable to post on a social media site, you should discuss it with your manager prior to posting.

Some typical examples of social media tools are blogs, wikis, social networking sites (such as Facebook, Instagram, LinkedIn and Twitter), podcasts and message boards.

Data Protection and Privacy

Tellus must hold and use certain information on living individuals to carry out its work and also to carry out various administrative functions both statutory and work related. The holding of this personal data, whether held on computers, paper or other media, is governed by local data protection laws.

Tellus endorses and complies with eight principles whereby personal data shall be:

- Fairly and lawfully processed
- Processed for limited purposes

- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure, and
- Not transferred to other countries without adequate protection

Tellus expects all those who work for it, either as staff or suppliers, to observe these principles in obtaining, handling, processing, transporting and storage of personal data.

Tellus Guidelines

- There will be limits to the collection of personal data and any such data will be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual
- Personal data will be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, will be accurate, complete and up to date; The purposes for which personal data are collected will be specified at the time of collection and the subsequent use limited to the fulfilment of those purposes
- Personal data will not be disclosed, made available or otherwise used for purposes other than those originally specified except with the consent of the individual or by authority of the law, and
- Personal data will be protected by reasonable security safeguards against risks such as loss or unauthorised access, destruction, use, modification or disclosure

Individual Guidelines

- Employees are responsible for ensuring that any personal data they hold is kept securely. They must also ensure that they do not disclose personal data either orally or in writing to any unauthorized third party
- Employees are responsible for checking that any personal data that they provide to Tellus is up to date and for informing the company of any changes to information that they have provided
- Employees are also responsible for checking any information that the company may send out from time to time, giving details of information that is being kept and processed, and
- Both employees, clients and candidates have the right to have any data relating to them communicated:
    - Within a reasonable time
    - At a charge, if any, that is not excessive
    - In a reasonable manner
    - In a form that is readily intelligible

If a request for data is denied, individuals will be given reasons and will be able to challenge such denial. Individuals have the right to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Approved by: Nathaniel Smith, Managing Director and CEO