DATA LOSS PREVENTION POLICY

1. **Introduction**

   This policy outlines the procedures that are to be implemented in order to prevent and mitigate data loss within Pangeotek Ltd.

2. **Scope**

   This policy applies to all employees, contractors and third-party personnel who have access to Pangeotek data.

3. **Objective**

   The objective of this policy is to ensure that data is securely stored and transmitted, and that any potential data loss incidents are rapidly detected and mitigated. It should further ensure that sensitive company data is protected from leaks, accidental loss, or unauthorised access. Here are the key procedures that should be followed:

4. **Procedures**

   - All data must be stored securely and with appropriate authentication and authorisation measures in place.
   - Devices used to access or store data must be password protected and regularly updated with the latest security patches.
   - Cloud based storage (Teams and One Drive) must be used to store all working files.
   - Data must be backed up regularly and securely stored in an off-site location.
   - Employee, contractor and third-party personnel must be trained on data loss. prevention procedures and regularly reminded of the importance of data security.
   - All personnel must use two-factor authentication when accessing data remotely.
   - Any suspected data loss incidents must be reported to the Management immediately.

5. **Enforcement**

   Failure to comply with this policy may result in disciplinary action.

Signed

Lee White
Director/Principal Consultant
Pangeotek Ltd

Last Reviewed 14th May 2026