DATA PROTECTION POLICY

1. INTRODUCTION

1.1 Everyone has rights with regard to the way in which their Personal Data is handled. During the course of its activities Tennants Consolidated Limited (the "**Company**") will collect, store and process personal data about its Company Personnel and other third parties, and the Company recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users ("You" or "you") are obliged to comply with this policy when processing personal data on the Company's behalf.

2. DEFINITIONS OF DATA PROTECTION TERMS

2.1 **Automated Decision-Making ("ADM")** is when a decision is made which is based solely on Automated Processing (including profiling) (that is, there is no meaningful human involvement in the taking of decision) and that decision produces legal effects or similarly significantly affects an individual. The **UK GDPR** prohibits Automated Decision-Making (unless certain conditions are met) when using Special Categories of Personal Data. Otherwise, the UK GDPR requires that certain safeguards are adopted when carrying out Automated Decision-Making.

2.2 **Company Personnel** are all employees, workers, contractors, agency workers, consultants, directors, members and others.

2.3 **Consent** is an agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

2.4 **Controller** is the person who or organisation which determines the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the UK GDPR. The Company is the Controller of all Personal Data used in the business for its own commercial purposes and relating to its Company Personnel.

2.5 **Data** is information which is stored electronically, on a computer, system or hosted environment, or in certain paper-based filing systems.

2.6 **Data Processor** is any person or organisation that is not a Controller that processes personal data on the Company's behalf and on the Company's instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the Company's behalf.

2.7 **Data Subjects** for the purpose of this policy include all living individuals about whom the Company hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

2.8 **Data Users** are those Company Personnel whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.9 **Explicit Consent** is consent which requires a very clear and specific statement (that is, not just action).

2.10 **Personal Data** means any information identifying a Data Subject or information relating to a Data Subject who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can

be an opinion about that person, their actions and behaviour (for example, as set out in an email). Personal Data includes Special Categories of Personal Data.

2.11 **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

2.12 **Privacy Notices or Privacy Policies** are separate notices setting out information provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the Company's Data Privacy Statement) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

2.13 **Processing (Process or Processed)** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

2.14 **Related Policies and Privacy Guidelines** are any of the Company's additional policies, operating procedures, guidelines or processes in place from time to time related to this Data Protection Policy, designed to protect Personal Data or which adhere to our data protection requirements.

2.15 **Special Categories of Personal Data** includes information about or recalling a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, sexual orientation, biometric or genetic data and Personal Data relating to criminal offences and convictions.

2.16 **UK GDPR** is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR and Data Protection Act. The Data (Use and Access) Act 2025 reforms certain aspects of the UK data protection regime; however, the core principles and overall legal framework under UK GDPR remain materially unchanged.

3. ABOUT THIS POLICY

3.1 This Data Protection Policy sets out how the Company handles the Personal Data of our customers, suppliers, employees, workers and other third parties.

3.2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

3.3 This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory.

3.4 The Company takes a strict approach to breaches of this policy which will be dealt with in accordance with the Company's Disciplinary Procedure. Any serious breach of this policy may amount to gross misconduct resulting in dismissal.

3.5 This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation.

3.6 This policy does not set terms or conditions of employment or form part of any employee's contract of employment and may be amended at any time.

3.7 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Group Company Secretary (Hannah.Gibson@tg-tcl.com).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 The Company adheres to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

4.1.1 Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

4.1.2 collected only for specified, explicit and legitimate purposes (purpose limitation);

4.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

4.1.4 accurate and where necessary kept up to date (accuracy);

4.1.5 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

4.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

4.1.7 not transferred to another country without appropriate safeguards in place (transfer limitation); and

4.1.8 made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts the Company's actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that the Company Processes Personal Data fairly and without adversely affecting the Data Subject.

5.3 The UK GDPR allows Processing of Personal Data by the Controller when it has a lawful ground to Process it. The key lawful grounds relied on by the Company are set out below:

5.3.1 the Data Subject has given his or her Consent;

5.3.2 the Processing is necessary for the performance of a contract with the Data Subject;

5.3.3 to meet the Company's legal compliance obligations; or

5.3.4 to pursue the Company's legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

The lawful grounds for which the Company processes Personal Data need to be set out in applicable Privacy Notices or Privacy Policies.

6. CONSENT

6.1 A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent (as mentioned in the previous section).

6.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.4 Usually, the Company will be relying on another legal basis (and not require Consent) to Process most types of Personal Data.

6.5 Where relying on Consent, You will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

7. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

7.1 The UK GDPR requires Controllers to provide certain, sufficiently detailed, information to Data Subjects whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Privacy Policies which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2 Whenever the Company collects Personal Data from Data Subjects, including for providing services to its clients, managing day-to-day business relations, or employment purposes, the Company must make available to the Data Subject all the information required by the UK GDPR including the identity of the Controller, how and why the Company will use, Process, disclose, protect and retain that Personal Data, the lawful bases for its uses and the Data Subject's rights under data protection laws. Such information is commonly set out in a Privacy Notice which must be appropriately made available to the Data Subject.

8. PURPOSE LIMITATION

8.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

8.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary (or the Company is able to rely on an appropriate lawful ground).

9. DATA MINIMISATION

9.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

9.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

9.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

10. ACCURACY

10.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected, updated or deleted without delay when inaccurate.

10.2 You will ensure that the Personal Data the Company uses and holds is accurate, complete, kept up to date and relevant to the purpose for which the Company collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. STORAGE LIMITATION

11.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

11.2 The Company will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law or certain exceptional circumstances communicated by the Company require that data to be kept for an additional time. You must comply with the Company's Data Retention Policy.

11.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which the Company originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

11.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that the Company no longer requires in accordance with all the Company's applicable records, retention schedules and policies. This includes requiring third parties to delete such data where applicable.

11.5 The Company will need to ensure Data Subjects are appropriately informed about the criteria used to determine how long Personal Data is stored in any applicable Privacy Notice or Privacy Policy.

12. DATA SECURITY

12.1 The Company will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, decimation or damage to, Personal Data.

12.2 The Company will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of

Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

12.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

12.4 You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Company's central computer system instead of individual PCs.

13. REPORTING A PERSONAL DATA BREACH

13.1 The UK GDPR requires Controllers to notify any Personal Data Breach:

13.1.1 to the UK Information Commissioner's Office **within 72 hours** of becoming aware (unless the Personal Data Breach is unlikely to result in a risk to the privacy of Data Subjects in which case notification to the ICO is not required); and

13.1.2 where there is a likelihood of high risk to the privacy of Data Subjects, to the Data Subjects themselves without undue delay.

13.2 The Company has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where the Company is legally required to do so.

13.3 If you know or suspect that a Personal Data Breach has occurred, **do not** attempt to investigate the matter yourself or disclose details about the incident to anyone outside the business. Immediately contact the Group Company Secretary (Hannah.Gibson@tg-tcl.com). You should preserve all evidence relating to the potential Personal Data Breach. You will need to provide all assistance requested and promptly, including providing all necessary information about the Personal Data Breach to the Group Company Secretary (or to whoever they instruct).

14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

14.1 The Company may share Personal Data the Company holds with any member of its corporate group.

14.2 The Company may also disclose Personal Data the Company holds to third parties if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Statement provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions;

(e) a fully executed written contract that contains UK GDPR approved third party clauses has been obtained; and

(f) the Company is under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others

15. INTERNATIONAL TRANSFERS LIMITATION

15.1 The UK GDPR places restrictions on data transfers to countries outside the UK not deemed to ensure an adequate level of data protection without appropriate safeguards. This is to ensure that the level of data protection afforded to individuals by the UK GDPR is not lowered. An international transfer of Personal Data is made when you transmit or send the Personal Data to a company in another country, or make it available for accessing or viewing by another company in a different country.

15.2 You may only transfer Personal Data outside the UK if one of the following conditions applies:

15.2.1 the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

15.2.2 appropriate safeguards are in place such as standard contractual clauses (entered into with the data recipient) approved for use in the UK and an accompanying transfer risk assessment has been completed;

15.2.3 the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

15.2.4 the transfer is necessary for one of the exceptions set out in the UK GDPR including:

15.2.4.1 the performance of a contract between us and the Data Subject;

15.2.4.2 reasons of public interest;

15.2.4.3 to establish, exercise or defend legal claims;

15.2.4.4 to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and

15.2.4.5 in some limited cases, for our legitimate interest.

16. DATA SUBJECT'S RIGHTS AND REQUESTS

16.1 Data Subjects have rights when it comes to how the Company handles their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Controller's Processing activities;

(c) request access to their Personal Data that the Company holds;

(d) object to the Company's use of their Personal Data for direct marketing purposes;

(e) ask the Company to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or for other specific reasons;

(f) rectify inaccurate data or to complete incomplete data;

(g) restrict Processing in specific circumstances;

(h) object to Processing which has been justified on the basis of the Company's legitimate interests or in the public interest;

(i) challenge decisions based solely on Automated Processing, including profiling (ADM);

(j) make a complaint to the supervisory authority (in the UK, it is the Information Commissioner's Office); and

(k) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

16.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

16.3 In any case, you must **immediately** forward any Data Subject request or data protection-related complaint you receive to the Group Company Secretary (Hannah.Gibson@tg-tcl.com) and **no later than 48 hours** from receipt of the request.

17. ACCOUNTABILITY

17.1 The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

17.2 The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

17.2.1 appointing a suitably qualified DPO where necessary or otherwise an executive accountable for data privacy;

17.2.2 implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

17.2.3 integrating best data protection practices into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines and Privacy Notices;

17.2.4 regularly training Company Personnel on the UK GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

17.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

18. RECORD KEEPING

18.1 The UK GDPR requires the Company to keep full and accurate records of all the Company's data Processing activities.

18.2 These records should include, at a minimum, the name and contact details of the Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

18.3 For further details regarding the keeping of these records, please contact our Group Company Secretary.

19. TRAINING AND AUDIT

19.1 The Company is required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. The Company must also regularly test its systems and processes to assess compliance.

19.2 When asked, you must promptly undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

19.3 You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

20. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

20.1 The Company is required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

20.2 You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

20.2.1 the state of the art;

20.2.2 the cost of implementation;

20.2.3 the nature, scope, context and purposes of Processing; and

20.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

20.3 The Controller must also conduct DPIAs in respect of any envisaged Processing likely to result in a high risk to the rights and freedoms of Data Subjects.

20.4 You should conduct a DPIA (and discuss your findings with Group Company Secretary (Hannah.Gibson@tg-tcl.com)) when implementing major system or business change programs involving the Processing of Personal Data including:

20.4.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

20.4.2 Automated Processing including profiling and ADM;

20.4.3 large scale Processing of Special Categories of Personal Data; and

20.4.4 large scale, systematic monitoring of a publicly accessible area.

20.5 A DPIA must include:

20.5.1 a description of the Processing, its purposes and the Controller's legitimate interests if appropriate;

20.5.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

20.5.3 an assessment of the risk to individuals; and

20.5.4 the risk mitigation measures in place and demonstration of compliance.

21. AUTOMATED DECISION-MAKING (ADM)

21.1 Generally, sole reliance on ADM is prohibited when the decision is based entirely or partly on processing Special Categories of Personal Data and has a legal or similar significant effect on the Data Subject unless:

21.1.1 that Data Subject has Explicitly Consented; or

21.1.2 the Processing is authorised by law or is necessary for the performance of or entering into a contract between the Controller and Data Subject and is necessary for reasons of substantial public interest in accordance with UK data protection laws.

21.2 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be appropriately informed (see the 'Transparency' section further above). As part of this, the Company must inform the Data Subject of the logic involved in the decision making or profiling, and the significance and envisaged consequences of the decision-making. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests. This includes allowing the Data Subject to make representations about, obtain human intervention by the Controller in relation to, and contest, such decisions.

21.3 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

21.4 For further details regarding this section, particularly if you are considering implementing Automated Processing or ADM, please contact our Group Company Secretary

22. DIRECT MARKETING

22.1 The Company is subject to certain rules and privacy laws when engaging in direct marketing to its customers and prospective customers (in particular, when sending marketing emails).

22.2 In a business-to-consumer context (and 'consumers', for these purposes, include sole traders and partnerships), the individual's prior consent is generally required for electronic direct marketing (for example, by email or text). The limited exception for existing consumers known as "soft opt-in" allows an organisation to send marketing emails without consent if it: (a) has obtained

the consumer's contact details in the course of a sale to that person; (b) is marketing similar products or services; and (c) gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.

22.3 The rules around email marketing are relatively more flexible for business-to-business marketing (that is, marketing to corporate entities) but we must ensure that we have an appropriate lawful ground and allow recipients to unsubscribe (see below).

22.4 The right to object to direct marketing must be explicitly offered to every Data Subject in every marketing communication.

22.5 A Data Subject's objection to direct marketing (that is, their unsubscribe request) must be promptly honoured. If a Data Subject opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

23. COMPLAINTS

23.1 Where the Company receives a complaint from a Data Subject relating to the Processing of their Personal Data, we will need to acknowledge receipt of the complaint no later than 30 days from when we received the complaint and, without undue delay, take appropriate steps (making enquiries into the subject matter of the complaint, to the extent appropriate) to respond to the complaint, keeping the Data Subject up-to-date on the progress and informing them of the outcome of the complaint.

23.2 In any case, you must **immediately** forward any Data Subject request or data protection-related complaint you receive to the Group Company Secretary (Hannah.Gibson@tg-tcl.com) and **no later than 48 hours** from receipt of the request.

24. CHANGES TO THIS POLICY

24.1 The Company may update this policy from time to time.

24.2 This policy does not override any applicable rational data privacy laws and regulations in countries where the Company operates (certain countries may have localised variances to this policy which are available on request to Group Company Secretary (Hannah.Gibson@tg-tcl.com).