Corporate Governance Plan

Way 2 Vat Limited

Table of contents

Schedule 1

Board Charter

Way 2 Vat Limited

(Company)

1 Role of the Board

1.1 This Board Charter details the principles for the operation of the board of directors of the Company (**Board**) and describes the functions of the Board.

1.2 The Board is accountable to shareholders for the performance of the Company. The Board must at all times act honestly, conscientiously and fairly in all respects in accordance with the law applicable to the Company and must act in the best interests of the Company's shareholders and other stakeholders.

1.3 The Board's role includes guiding the Company's strategic direction, driving its performance and overseeing the activities of management and the operation of the Company.

1.4 This Board Charter and the charters adopted by the Board for the committees established by the Board have been adopted on the basis that good corporate governance adds to the performance of the Company and creates shareholder value and engenders the confidence of the investment market.

2 Responsibilities of the Board

The Board is responsible for managing the affairs of the Company, including to:

(a) **Strategic and financial performance**

(i) provide leadership and develop and approve the Company's corporate strategy, investment and performance objectives;

(ii) evaluate, approve and monitor the Company's strategic, investment and financial plans and objectives;

(iii) evaluate, approve and monitor the annual budgets and business plans;

(iv) determine the Company's dividend policy (if any), dividend re-investment plan (if any) and the amount and timing of all dividends;

(v) evaluate, approve and monitor major capital expenditure, capital management and all major acquisitions, divestitures and other corporate transactions, including the issue of securities of the Company;

(vi) approve all accounting policies, financial reports and material reporting and external communications by the Company;

(vii) assess the solvency and performance of the Company;

(viii) appoint the Chair of the Board and, where appropriate, any deputy chairperson or senior independent director, in accordance with to the Company's articles of association, as amended from time to time (**Articles**) and applicable law;

(b) **Executive management**

(i) appoint, monitor and manage the performance of the Company's executive directors;

(ii) manage succession planning for the Company's executive directors and any other key management positions as identified from time to time, including reviewing any succession plans recommended by the Remuneration and Nomination Committee (if any);

(iii) appoint and, where appropriate, remove any Chief Executive Officer, in accordance with the Articles;

(iv) ratify the appointment and, where appropriate, the removal of senior management of the Company and any subsidiaries;

(v) with the advice and assistance of the Remuneration and Nomination Committee (if any), review and approve the performance of individual Board members and senior executives as well as any policies concerned with the remuneration of any employee;

(vi) with the advice and assistance of the Remuneration and Nomination Committee (if any), review and approve, subject to other corporate approvals as required in accordance with applicable law, the remuneration of individual Board members and senior executives, having regard to their performance;

(vii) ensure appropriate resources are available to senior executives;

(viii) advise senior management of its obligation to provide to the Board all information required by it to discharge its responsibilities, including any information specifically requested by the Board;

(ix) oversee senior management's implementation of the Company's strategic objectives;

(c) **Audit and risk management**

(i) with the recommendation of the Risk and Audit Committee (if any), appoint the external auditor and determine its remuneration and terms of appointment, subject to the Articles and other corporate approvals as required in accordance with applicable law;

(ii) ensure effective audit, risk management and regulatory compliance programs are in place to protect the Company's assets and shareholder value;

(iii) evaluate, establish, approve and monitor the risk appetite within which the Board expects management of the Company to operate;

(iv) approve and monitor the Company's risk and audit framework, including (but not limited to) systems of risk management and internal compliance and control;

(v) approve and, with the assistance and advice of the Risk and Audit Committee (if any), monitor compliance with the Company's Risk Management Policy (if any);

(vi) monitor the Company's operations in relation to, and in compliance with, relevant regulatory and legal requirements;

(vii) approve and oversee the integrity of the accounting, financial and other corporate reporting systems and monitor the operation of these systems;

(viii) with the recommendation of the Risk and Audit Committee (if any), review and approve a process by which the integrity of any periodic corporate report released to the market that is not audited or reviewed by the an external auditor can be verified;

(d) **Strategic planning**

(i) engage in strategic planning including establish goals for management of the Company and monitor the achievement of those goals;

(ii) ensure strategic planning is based on the identification of opportunities and the full range of business risks that will determine which of those opportunities are most worth pursuing;

(iii) on an ongoing basis, review how the strategic environment is changing, what key business risks and opportunities are appearing, how they are being managed and what, if any, modifications in strategic direction should be adopted;

(e) **Corporate governance and disclosure**

(i) oversee the affairs of the Company, including its control and accountability systems;

(ii) evaluate the overall effectiveness of the Board, its committees and its corporate governance practices;

(iii) at least once each year review the performance and effectiveness of the Company's corporate governance policies and procedures and, if appropriate, amending those policies and procedures or adopting new policies or procedures;

(iv) review and approve all disclosures related to any departures from the Corporate Governance Principles and Recommendations of the ASX Corporate Governance Council;

(v) review and approve the public disclosure of any Company policy or procedure;

(vi) supervise the public disclosure of all matters that the law and the ASX Listing Rules require to be publicly disclosed in a manner consistent with the Continuous Disclosure Policy;

(vii) develop and review an appropriate communications policy to promote effective communication with shareholders and participation at general meetings;

(viii) disclose the process by which the integrity of any periodic corporate report the Company releases that is not audited or reviewed by an external auditor is verified;

(ix) approve, subject to other corporate approvals as required in accordance with applicable law, the appointment of directors to committees established by the Board and oversee the conduct of each committee;

(x) approve and monitor delegations of authority, subject to applicable law;

(xi) with the assistance of the Remuneration and Nomination Committee (if any), identify any specific responsibilities of individual Board members, including the Chairperson;

(xii) prepare the Company's annual corporate governance disclosure statements as required under the ASX Listing Rules;

(f) **Performance evaluation**

(i) at least once per year, with the advice and assistance of the Remuneration and Nomination Committee (if any), review and evaluate the performance of the Board, each board committee, and each individual director against the

relevant charters, corporate governance policies, and agreed goals and objectives;

(ii) following each review and evaluation, consider how to improve performance;

(iii) agree and set the goals and objectives for the Board and its committees each year, and if necessary, amending the relevant charters, committees, policies or goals and objectives;

(iv) with the advice and assistance of the Remuneration and Nomination Committee (if any), review and approve, subject to other corporate approvals as required in accordance with applicable law, the remuneration of the Company's executive and non-executive directors;

(v) disclose the process for periodically evaluating performance and whether, for each reporting period, a performance evaluation occurred;

(g) **Code of Conduct and Ethics**

(i) adopt and apply appropriate ethical standards in relation to the management of the Company and the conduct of its business; and

(ii) monitor compliance with the Company's Code of Conduct and Ethics; and

(iii) ensure that the Board or the Remuneration and Nomination Committee is informed of any material breaches of the Company's Code of Conduct and Ethics.

3 Structure of the Board

The Board shall comprise of such number of members as shall be determined in the Articles from time to time and it is intended that the Board should, to the extent practicable given the size and composition of the Board from time to time, be comprised of a majority of independent directors. The Board aims to comprise directors with a broad range of skills, expertise, and experience from a diverse range of backgrounds that is appropriate to the Company and its strategy.

4 Independent Director

4.1 Where this Charter or the charter of a board committee requires one or more 'independent' directors, the following criteria are to be applied.

4.2 An 'independent' director is an 'External Director' according to the Israeli Companies Law as well as a non-executive director who:

(a) is not a substantial shareholder (as defined in the *Corporations Act 2001* (Cth)) of the Company or an officer of, or otherwise associated with, a substantial shareholder of the Company;

(b) within the last three years, has not been employed in an executive capacity by the Company or any of its subsidiaries, or been a director after ceasing to hold any such employment;

(c) within the last three years has not been a partner, director or senior employee of a provider of material professional services to the Company or any of its subsidiaries;

(d) within the last three years has not been in a material business relationship (eg. a material supplier or customer) with the Company or any of its subsidiaries, or an officer of, or otherwise associated with, someone with such a relationship;

(e) has no material contractual relationship with the Company or any of its subsidiaries other than as a director of the Company;

(f) do not have close family ties with any person who falls within any of the categories described above;

(g) has not served on the Board for a period which could, or could reasonably be perceived to, materially interfere with the director's capacity to bring an independence judgement to bear on issues before the Board and the director's ability to act in the best interests of the Company and its shareholders generally; and

(h) is free from any interest and any business or other relationship which could, or could reasonably be perceived to, materially interfere with the director's capacity to bring an independence judgement to bear on issues before the Board and the director's ability to act in the best interests of the Company and its shareholders generally.

4.3 Family ties and cross-directorships may be relevant in considering interests and relationships which may compromise independence and should be disclosed by directors to the Board.

4.4 The Board should regularly assess whether each non-executive director is independent. Each non-executive director should provide to the Board all information that may be relevant to this assessment. If a director's independent status changes, this should be disclosed and explained to the market in a timely manner.

5 Directors' Responsibilities

5.1 Each director of the Company is bound by the Company's charters and policies, including any of the following policies adopted by the Board:

(a) Securities Trading Policy;

(b) Continuous Disclosure Policy;

(c) Risk and Audit Committee Charter;

(d) Remuneration and Nomination Committee Charter;

(e) Diversity Policy;

(f) Risk Management Policy;

(g) Code of Conduct and Ethics; and

(h) Shareholder Communications Policy; and

(i) Anti-Bribery and Anti-Corruption Policy.

5.2 The Board may adopt additional policies as required based on the Company's size and operations from time to time.

5.3 The directors of the Company must:

(a) conduct their duties at the highest level of honesty and integrity;

(b) observe the rule and the spirit of the laws to which the Company is bound and comply with any relevant ethical and technical standards;

(c) maintain the confidentiality of all information acquired in the course of conducting their role and not make improper use of, or disclose to third parties, any confidential information unless that disclosure has been authorised by the Board or is required by law or by the ASX Listing Rules;

(d) observe the principles of independence, accuracy and integrity in dealings with the Board, board committees, internal and external auditors, senior management and employees within the Company;

(e) act in accordance with this Board Charter and disclose to the Board any actual or perceived conflicts of interest, whether of a direct or indirect nature, of which the director becomes aware and which the director reasonably believes is material, in that it may or may be perceived to influence his vote or compromise the reputation or performance of the Company; and

(f) set a standard of honesty, fairness, integrity, diligence and competency in respect of the position of director.

6 Role of the Chairperson

6.1 The Company recognises that it is important that the Chairperson has a defined role in the organisation and operates in accordance with clear functional lines.

6.2 The role of Chairperson requires a significant time commitment. The Chairperson's other positions should not be such that they are likely to hinder effective performance in the role.

7 Specific Duties of the Chairperson

7.1 The Chairperson will:

(a) where practicable, be an independent non-executive director and where the Chairperson is not an independent director, the Company will appoint a lead independent director if it is practicable to do so. The lead independent director will take over the role of the Chairperson when the Chairperson is unable to act in that capacity as a result of his or her lack of independence;

(b) chair board meetings;

(c) establish the agenda for Board meetings, in consultation with the directors and the Company Secretary; and

(d) chair meetings of shareholders, including the Annual General Meeting of the Company.

7.2 The roles of Chairperson and Chief Executive Officer (if any) will be exercised by two separate individuals.

7.3 The Chairperson will be selected on the basis of relevant experience, skill, judgement and leadership abilities to contribute to the effective direction of the Company.

7.4 The Chairperson is responsible for:

(a) leadership of the Board and for the efficient organisation and conduct of the Board's functions;

(b) promoting a constructive governance culture and applying appropriate governance principles among directors and with management; and

(c) facilitating the effective contribution of all directors and promoting constructive and respectful relations between directors and between Board and management.

7.5 The Chairperson must ensure that all substantive resolutions at a meeting of security holders must be decided by a poll rather than by a show of hands.

8 Specific Duties of the Chief Executive Officer or Managing Director

8.1 The Board will delegate to the Chief Executive Officer or Managing Director the authority and power to manage the Company and its business within levels of authority specified by the Board from time to time. The Chief Executive Officer may delegate aspects of his or her authority and power to other senior executives but remains accountable to the Board for the day to day management of the Company. The Chief Executive Officer's or Managing Director's role includes:

(a) responsibility for the effective leadership of the management team;

(b) the development of strategic objectives for the business; and

(c) the day to day management of the Company.

9 Confidential Information and External Communication

The Board has established the following principles to apply in respect of information of the Company:

(a) generally, the Chairperson will speak for the Company. Individual Board members are expected not to communicate on behalf of the Board or the Company without prior consultation with the Chairperson;

(b) any disclosure of information to a shareholder which is not disclosed to the market must be approved under the Continuous Disclosure Policy and must comply with the ASX Listing Rules; and

(c) all directors are required to keep all information provided to them in their capacity as a director confidential, unless it is required by law or by the ASX Listing Rules.

10 Conflicts of Interest

10.1 The directors of the Company are required to act in a manner which is consistent with the best interests of the Company as a whole, free of any actual or possible conflicts of interest.

10.2 If a director considers that they might be in a position where there is a reasonable possibility of conflict between their personal or business interests, the interests of any associated person, or their duties to any other company, on the one hand, and the interests of the Company or their duties to the Company, on the other hand, the director must:

(a) fully and frankly inform the Board about the circumstances giving rise to the possible or actual conflict;

(b) if requested by the Board, within seven days or such further period as may be permitted by the Board, take such steps necessary and reasonable to remove any conflict of interest; and

(c) abstain from voting on any motion relating to the matter and absent themself from all board deliberations relating to the matter, including receipt of Board papers bearing on the matter.

10.3 If a director believes that they may have a conflict of interest or duty in relation to a particular matter, the director should immediately consult with the Chairperson (or, in the case of the Chairperson, the Chairperson should immediately consult with the other non-executive directors).

11 Related Party Transactions

11.1 If established, the Board delegates to the Risk and Audit Committee responsibility for reviewing and monitoring, subject to applicable law, related party transactions and investments involving the Company and its directors.

12 Meetings

12.1 The Board will meet regularly on such number of occasions each year as the Board deems appropriate.

12.2 A meeting of the Board will usually be convened by the Chairperson.

12.3 All directors are expected to diligently prepare for, attend and participate in all Board meetings. At a minimum, a quorum of directors under the Company's articles of association is a majority of the directors then in office. Meetings of the Board may be held or participated in by conference call or similar means. Resolutions of the Board may be passed by circular resolution or in writing in accordance with the Company's articles of association.

12.4 The Chairperson should ensure the availability and, if necessary, the attendance at the relevant meeting, of any member of the Company's executive management responsible for a matter included as an agenda item at the relevant meeting.

13 Agenda

13.1 An agenda will be prepared for each Board and Board committee meeting. The agenda will be prepared by the Company Secretary.

13.2 The following items will be standing items on the agenda unless otherwise determined by the Chairperson:

(a) approval of minutes of previous Board meeting;

(b) matters arising from minutes of previous Board meeting (Note: directors are expected to review the minutes carefully and raise any concerns, requested amendments or seek clarification in the following Board meeting);

(c) consideration of any continuous disclosure matters;

(d) directors' declarations; and

(e) items requiring Board approval.

14 Board Committees

14.1 Once the Board is of a sufficient size and structure, and the Company's operations are of a sufficient size, to assist the Board in fulfilling its duties, the Board may establish the following committees, subject to applicable law:

(a) the Risk and Audit Committee, which is responsible for monitoring and advising the Board on the Company's audit, risk management and regulatory compliance policies and procedures; and

(b) the Remuneration and Nomination Committee, which is responsible for establishing the policies and practices of the Company regarding the remuneration of directors and other senior executives and reviewing all components of the remuneration framework, advising the Board on the composition of the Board and its committees, reviewing the performance of the Board, its committees and the individual directors, ensuring the proper succession plans are in place and advising the Board in respect of the

effectiveness of its corporate governance policies and developments in corporate governance.

14.2 Although the Board may delegate powers and responsibilities to these committees, subject to applicable law, the Board retains ultimate accountability for discharging its duties.

14.3 The composition of the membership, including the Chairperson, of each of these committees will be as determined by the Board from time to time, subject to the following restrictions:

(a) the Risk and Audit Committee must comprise at least three members, including all External Directors, and the majority of whom will be independent; and

(b) the Remuneration and Nomination Committee must comprise at least three members, including all external directors, and the majority of whom will be independent directors.

14.4 The Board will consider and approve the charters of the various committees. These Charters will identify the areas in which the Board will be assisted by each committee. Each committee will report regularly to the Board in accordance with their respective charters.

14.5 The Board must disclose:

(a) the charters of each committee;

(b) the members of the Remuneration and Nomination Committee;

(c) the members of the Risk and Audit Committee and their relevant qualifications and experience;

(d) at the end of each reporting period:

(i) the number of times each committee met throughout the period and the individual attendances of the members at those meetings;

(ii) whether a review of the Company's risk management framework has been reviewed.

14.6 The Board may establish other committees as and when required.

15 Company Secretary

15.1 The Company Secretary is directly accountable to the Board through the Chairperson, unless delegated by the Board to another appropriate person. The company secretary's role is to:

(a) advise the Board and its committees on governance matters;

(b) coordinate all Board business including:

(i) prepare agendas;

(ii) coordinate the timely completion and despatch of Board and committee papers;

(iii) ensure the business at Board and committee meetings is accurately captured in the minutes;

(iv) lodge communications and filings with the ASX;

(v) monitor compliance with Board and committee policy and procedures; and

(vi) help to organise and facilitate the induction and professional development of directors.

15.2 The Board will appoint at least one company secretary. Appointment and removal of a company secretary will be subject to Board approval.

15.3 All directors will have direct access to the company secretary.

16 Independent Advice

16.1 A director of the Company is entitled to seek independent professional advice (including, but not limited to, legal, accounting and financial advice) at the Company's reasonable expense on any matter connected with the discharge of his or her responsibilities, so long as he or she is acting reasonably in the interests of the Company and in the discharge of his or her duties as a director, in accordance with the procedures and subject to the conditions below:

(a) a director must seek the prior approval of the Chairperson;

(b) in seeking the prior approval of the Chairperson, the director must provide the Chairperson with details of the nature of the independent professional advice, the likely cost of the advice and details of the adviser he or she proposes to instruct;

(c) the Chairperson may set a reasonable limit on the amount that the Company will contribute towards the cost of obtaining the advice;

(d) all documentation containing or seeking independent professional advice must clearly state that the advice is sought both in relation to the Company and to the director in their professional capacity. However, the right to advice does not extend to advice concerning matters of a personal or private nature, including for example, matters relating to the director's contract of employment with the Company (in the case of an executive director) or any dispute between the director and the Company; and

(e) the Chairperson may determine that any advice received by an individual director will be circulated to the remainder of the Board.

16.2 All directors are entitled to the benefit of the Company's standard Deed of Access, Indemnity and Insurance which provides ongoing access to Board Papers and, at the Company's expense, Directors and Officers insurance.

17 Remuneration

The level of director remuneration will be approved by the Board and by shareholders as the Company's articles of association and applicable law may require.

18 Annual Review

18.1 The Board will review and prepare annually:

(a) a self-evaluation of its performance against this Charter;

(b) recommended goals and objectives for the coming year; and

(c) recommended changes or improvements to this Charter if necessary.

18.2 **Revisions of this Charter**

18.3 This Board Charter and any amendments to it must be approved by each director of the Company.

18.4 Each director is responsible for review of the effectiveness of this Charter and the operations of the Board and to make recommendations to the Board of any amendments to this Board Charter.

Schedule 2

Corporate Code of Conduct

Way 2 Vat Limited

(Company)

1 Objectives

1.1 This Code of Conduct has been established by the board of directors (**Board**) of the Company and applies to all Personnel of the Company. The Company is committed to complying with all applicable laws and regulations and to delivering strong returns and shareholder value while also promoting shareholder and general market confidence in the Company. The Company is also committed to acting ethically and responsibly in its dealings with third parties. The Code of Conduct is designed to establish the practices which are necessary to maintain confidence in the Company's integrity.

1.2 In this Code of Conduct, **Personnel** means a director (executive or non-executive), officer, employee, authorised representative, contractor or consultant of the Company or any subsidiary of the Company, if any.

1.3 The objectives of this Code of Conduct are to ensure that:

(a) high standards of corporate and individual behaviour are observed by all Personnel;

(b) Personnel are aware of their responsibilities to the Company; and

(c) all persons dealing with the Company, whether it be Personnel, shareholders, suppliers or competitors, can be guided by the stated values and practices of the Company.

1.4 The Company is committed to complying with this Code of Conduct and requires all Personnel to comply with it. Personnel must comply with both the spirit as well as the letter of all laws and regulations which apply to the Company and the principles of this Code of Conduct. Further, Personnel should always use due care and diligence when fulfilling their role or representing the Company and should not engage in any conduct likely to bring discredit upon the Company.

2 Conflicts of Interest

2.1 A conflict of interest occurs when a Personnel's interests interfere, or appear to interfere, with the Company's interests. The Company expects Personnel to act honestly, with high standards of personal integrity and in good faith at all times and, in a manner which is in the best interests of the Company as a whole and that would not negatively affect the Company's reputation.

2.2 Personnel will conduct their personal activities in a manner that is lawful and avoids possible, actual or perceived conflicts of interest between the Personnel's personal interests and those of the Company. Personnel (other than directors) must promptly disclosed to HR Manager any actual or potential conflict of interest of which they become aware. Directors (executive and non-executive) must promptly disclose to the Board any actual or potential conflict of interest of which they become aware.

3 Corporate Opportunities

Personnel will not:

(a) take advantage of the property or information of the Company or its customers, their position or opportunities arising from these, for personal gain or to cause detriment to the Company or its customers;

(b) use the Company's assets and property (including the Company's name) or information for any purposes other than lawful purposes authorised by the Board;

(c) enter into any arrangement or participate in any activity that would conflict with the Company's best interests or that would be likely to negatively affect the Company's reputation;

(d) disclose any of the Company's information, except where disclosure is permitted or required by the Company's articles of association, law or the ASX Listing Rules; or

(e) offer or accept bribes, inducements, commissions or misuse Company assets and resources.

4 Trading in Securities

Personnel will ensure that all trading in securities, including trading in securities of the Company, is in accordance with the Company's Securities Trading Policy. The purpose of the Securities Trading Policy is to ensure compliance with the law and to minimise the scope for misunderstandings or suspicions regarding Personnel trading in securities while in possession of non-public price sensitive information.

5 Confidentiality

5.1 Personnel will maintain and protect the confidentiality of the Company's information, except where disclosure is allowed by the Board or is required by law.

5.2 Personnel will not make improper use of any information acquired by virtue of being a Personnel of the Company, including the use of that information for personal gain or the gain of another party or in breach of a person's privacy.

6 Responsibilities to key stakeholders

6.1 Personnel will always deal with shareholders, customers, suppliers, competitors and other Personnel in a manner that is lawful, diligent and fair and with honesty, integrity and respect.

7 Compliance with applicable laws, regulations and rules

7.1 Personnel will always act in a manner that is compliant with all laws and regulations that apply to the Company and its operations.

7.2 Personnel will act in compliance with this Code of Conduct and the Company's other policies.

7.3 Personnel will not knowingly participate in any illegal or unethical activity.

7.4 Personnel shall report any actual or potential breaches of law, this Code of Conduct or the Company's other policies to the Company's Audit and Risk Committee. If ever in doubt, Personnel should seek advice immediately.

8 Employment Practices

The Company aims to provide a work environment in which all Personnel can excel regardless of race, religion, age, disability, gender, sexual preference or marital status. The Company will

from time to time maintain various policies relating to the workplace, including the Company's Diversity Policy. Personnel should familiarise themselves with these policies and ensure that they comply with them.

9 Reporting Concerns

9.1 The Company requires all Personnel who become aware of an actual or suspected violation of this Code of Conduct to report to HR Manager (**Reporting Person**). The Company will ensure that Personnel are not disadvantaged in any way for reporting violations of the Code of Conduct or other unlawful or unethical conduct and that matters are dealt with promptly and fairly.

9.2 Upon receipt and investigation of a notification of an actual or suspected violation of this Code of Conduct, the Reporting Person shall escalate the complaint for further investigation or action to the Chief Executive Officer or the Chairperson as appropriate depending on the nature and circumstances of the reported violation. The Board is informed of any material breaches of the Corporate Code of Conduct.

10 Compliance

10.1 The Board is responsible for monitoring compliance with this Code of Conduct. Any queries in relation to this Code of Conduct should be referred to HR Manager.

10.2 Failure by Personnel to comply with this Code of Conduct may result in disciplinary action, including in serious cases, the termination of engagement.

11 Review

This Code of Conduct is subject to periodic review by the Board.

Schedule 3

Risk and Audit Committee Charter

Way 2 Vat Limited

(Company)

1 Objectives

1.1 The Risk and Audit Committee (**Committee**) has been established by the board of directors (**Board**) of the Company pursuant to article 47 of the Company's articles of association. The Committee's primary objective is, in addition to its functions mandated by the Israeli Companies Law, 1999 (**Companies Law**), to facilitate the proper execution of the responsibilities of the Board relating to accounting and reporting practices of the Company.

1.2 The purpose of the Committee is to:

(a) oversee, review and supervise the Company's risk management framework and promote a risk management culture;

(b) assist the Board in discharging its responsibilities relative to the financial reporting process, the system of internal control relating to all matters affecting the Company's financial performance and the audit process;

(c) recommend to the shareholders of the Company to appoint and approve the compensation of the independent registered public accounting firm (external auditor) engaged to audit the Company's financial statements;

(d) oversee and monitor (i) the integrity of the Company's financial statements, (ii) the independent registered public accounting firm's qualifications, independence and performance, and (iii) the Company's internal accounting and financial controls;

(e) assist the Board in monitoring compliance with laws and regulations, especially as they relate to financial statements or accounting matters, and the Company's Code of Conduct and Ethics;

(f) provide to the Board such additional information and materials as it may deem necessary to make the Board aware of significant financial matters that require the attention of the Board;

(g) monitor deficiencies in the management of the Company, inter alia, in consultation with the internal auditor, and advise the Board on how to correct the deficiencies;

(h) decide whether to approve engagements or transactions that require Committee approval under the Companies Law, the *Corporations Act 2001* (Cth) (**Corporations Act**) (if applicable), and the ASX Listing Rules, relating generally to certain related party transactions;

(i) meet and receive reports from both the internal auditors and independent registered public accounting firm dealing with matters that arise in connection with their audits;

(j) assist the Board to adopt and apply appropriate ethical standards in relation to the management of the Company and the conduct of its business; and

(k) review the adequacy of the Company's insurance policies.

2 Authority

2.1 The Committee has authority to:

(a) conduct or authorise investigations into any matters within its purpose and have direct access to the independent registered public accounting firm as well as anyone in the organization;

(b) seek external advice or assistance, at the expense of the Company, including the appointment of consultants and independent external advice; and

(c) seek information and communicate directly with the Company's senior management, advisers, internal auditor (if appointed) and external auditor at any time.

2.2 The Committee will make recommendations to the Board on all matters requiring a decision from the Board. The Committee does not have the power or authority to make a decision in the Board's name or on its behalf.

3 Membership

3.1 Members of the Committee shall comprise directors appointed by the Board, as further detailed in Section 3.2 below.

3.2 The number of members of the Committee shall be a minimum of three directors, all of whom shall meet the following criteria (as well as any other criteria required by the ASX or the Companies Law):

(a) Each 'external director' appointed under the Companies Law (**External Director**) shall be a member of the Committee and at least one of such External Directors shall possess 'accounting and financial expertise' consistent with the Companies Law (and to the extent required by it);

(b) A majority of the members of the Committee shall be 'unaffiliated directors' (or 'independent directors') as defined in the Companies Law (**Unaffiliated Directors**);

(c) No member of the Committee may have participated in the preparation of the financial statements of the Company or any of the Company's current subsidiaries during the preceding three years; and

(d) Each member of the Committee must be able to read and understand fundamental financial statements (including a company's balance sheet, statement of operation and comprehensive income and statement of cash flows).

3.3 All members of the Committee shall be financially literate and the members of the Committee, between them, should have the accounting and financial expertise and a sufficient understanding of the industry in which the Company operates to be able to discharge the Committee's mandate effectively.

3.4 The Board will nominate the Chair of the Committee from time to time. The Committee Chair will be an who is not Chair of the Board.

3.5 Without limiting the foregoing, the following persons may not serve on the Committee:

(a) The Chair of the Board;

(b) Any person who is a holder of control (as defined in the Companies Law) or a relative of such a person; and

(c) Any person who is any relationship that, in the opinion of the Board, would interfere with the exercise of his or her independent judgment as a member of the Committee.

4 Committee Meetings

4.1 The Committee will meet, independently of the independent registered public accounting firm (external auditor), as often as the Committee members deem necessary to discharge its role effectively, but not less than twice a year having regard to the Company's reporting and financial audit cycle.

4.2 The Committee Chair shall convene a meeting of the Committee at any reasonable time or if required to do so by any Committee member or the Board. The internal auditor shall be invited to all Audit Committee meetings. In addition, the internal auditor may request that the Committee Chair convene a meeting to discuss a particular issue, and the Chair shall convene the Committee within a reasonable period of time, if the Chair finds it appropriate to do so.

4.3 A quorum of the Committee will comprise a majority of the members of the Committee, and the act of a majority of those present at any meeting at which there is a quorum shall be the act of the Committee, provided, however, that the majority of those members present shall qualify as Unaffiliated Directors and that at least one of those Unaffiliated Directors present shall be an External Director.

4.4 The Committee, in its discretion, will ask members of management or others to attend its meetings (or portions thereof) and to provide pertinent information as necessary. The Committee will meet separately with the Chief Executive Officer and separately with the Chief Financial Officer of the Company at such times as are appropriate to review the financial affairs of the Company.

4.5 If the Committee Chair is absent from a meeting and no acting chair has been appointed, the Committee members present may choose one of them to act as chair for that meeting.

4.6 Reasonable notice of meetings and the business to be conducted shall be given to the members of the Committee and any other person invited by the Committee to attend.

4.7 Meetings of the Committee may be held or participated in by conference call or similar means, and decisions may be made by circular or written resolution.

4.8 Each member of the Committee will have one vote. The Committee Chair will not have a casting vote. If there is a tied vote, the motion will be referred to the Board for resolution.

4.9 Following each meeting, the Committee Chair will report to the Board, at the next Board meeting, on any matter that should be brought to the Board's attention and on any recommendation of the Committee that requires Board approval or action, and provide the Board with sufficient information upon which to make a decision in that regard.

4.10 The Company Secretary shall co-ordinate the timely completion and dispatch of the Committee agenda, minutes and materials for each meeting. The minutes of each Committee meeting will, following preliminary approval by the Committee Chair, be circulated to the Board.

5 Responsibilities

The responsibilities of the Committee are as follows:

(a) **Risk management**

(i) consider the overall risk management framework and risk profile and annually review its effectiveness in meeting sound corporate governance principles and keep the Board informed of all significant business risks;

(ii) review with management the adequacy of the Company's systems for identifying, managing, and monitoring the key risks to the Company in accordance with the Company's Risk Management Policy;

(iii) obtain reports from management on the status of any key risk exposures or incidents;

(iv) review the adequacy of the Company's process for managing risk and provide a recommendation to the Board regarding the same in accordance with the Company's Risk Management Policy;

(v) review any incident involving fraud or other break down of the Company's internal controls in accordance with the Company's Risk Management Policy;

(vi) review any incident involving any break down of the Company's risk management framework in accordance with the Company's Risk Management Policy;

(vii) review the Company's insurance program having regard to the Company's business and the insurable risks associated with its business and inform the Board regarding the same;

(viii) review whether the Company has any material exposure to any economic, environmental and social sustainability risks and if so, develop strategies to manage such risks to present to the Board;

(b) **Financial statements**

(i) review the half-yearly and yearly financial statements and consider whether they are complete, consistent with information known to the Committee, reflect appropriate accounting policies and principles and otherwise provide a true and fair view of the financial position and performance of the Company;

(ii) receive and consider in connection with the Company's half-yearly and yearly financial statements letters of representation to the Board in respect of financial reporting and the adequacy and effectiveness of the Company's risk management, internal compliance and control systems and the process and evidence adopted to satisfy those conclusions;

(iii) review the financial sections of the Company's Annual Report and related regulatory filings before release and consider the accuracy and completeness of the information;

(iv) review with management and the external auditors the results of the audit;

(v) receive from the Company Chief Executive Officer and Chief Financial Officer a declaration that, in their opinion, the financial records of the Company have been properly maintained and that the financial statements comply with accounting standards and give a true and fair view of the financial position and performance of the Company and that the opinion has been formed on the basis of a sound system of risk management and internal control which is operating effectively before the Board approves the half-yearly and yearly financial statements;

(vi) review, in conjunction with counsel, any legal matters that could have a significant impact on the Company’s financial statements;

(c) **Internal control**

(i) monitoring of corporate risk assessment and the internal controls instituted in accordance with the Company's Risk Management Policy;

(ii) review the effectiveness of the Company’s internal controls regarding all matters affecting the Company’s financial performance and financial reporting, including information technology security and control;

(iii) review the scope of internal (if one is appointed) and external auditors’ review of internal control, review reports on significant findings and

recommendations, together with management's responses, and recommend changes from time to time as appropriate;

(d) **Internal audit**

(i) review with management and the internal auditor (if one is appointed) the plans and activities of the internal auditor;

(ii) meet with the internal auditor (if one is appointed) to review reports and monitor management response;

(iii) review the scope and adequacy of the internal audit work plan (if any);

(iv) meet separately, at least once a year, to discuss any matters that the Committee or internal auditor (if one is appointed) believes should be discussed privately;

(v) review the objectivity and performance of the internal audit activity (if any);

(vi) review the independence of the internal auditors (if any) and their auditing practices;

(vii) ensure there are no unjustified restrictions or limitations placed on the internal audit function, and review and concur in the appointment, replacement or dismissal of the internal auditor (if one is appointed);

(e) **External audit**

(i) establish procedures for the selection, appointment and removal of the external auditor and for the rotation of external audit engagement partners;

(ii) review the external auditors' proposed audit scope and approach;

(iii) meet with the external auditor to review reports, and meet separately from management, at least once a year, to discuss in that regard any matters that the Committee or auditors believe should be discussed privately;

(iv) establish policies as appropriate in regards to the independence, integrity and performance of the external auditor;

(v) review of the independence of the external auditors and the appropriateness of any services provided by them to the Company (if any), outside their statutory role;

(vi) for the purpose of removing or appointing external auditors review their performance, including their proposed fees, and if appropriate conduct a tender of the audit. Any subsequent recommendation following the tender for the appointment of an external auditor will be put to the Board and then if a change is approved it will be put forward to shareholders for their approval;

(vii) review any proposal for the external auditor to provide non-audit services and consider whether it might compromise the independence of the external auditor;

(f) **Compliance**

(i) consider the workplan for Company compliance activities;

(ii) obtain regular updates from management regarding compliance matters;

(iii) review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up (including disciplinary action) of any instances of non-compliance;

(iv) review and assess the management process supporting external reporting;

(v) review the findings of any examinations by regulatory agencies and authorities;

(vi) review the process for communicating the Code of Conduct and Ethics to Company personnel, and for monitoring compliance with that Code;

(g) **Reporting responsibilities**

(i) regularly report to the Board about Committee activities, issues, and related recommendations. Such report should include the results of the Committee's:

(A) assessment of whether external reporting is consistent with Committee members' information and knowledge and is adequate for the needs of the Company's shareholders;

(B) assessment of the management processes which supports external reporting;

(C) assessment of the Company's corporate reporting processes;

(D) assessment of the appropriateness of the accounting choices made by management in preparing the Company's financial statements;

(E) procedures for the selection and appointment of the Company's external auditor and for the rotation of external audit engagement partners;

(F) recommendations for the appointment or, if necessary, the removal of the external auditor;

(G) assessment of the performance and independence of the Company's external auditor. Where the external auditor provides non-audit services, the report should also state whether the Committee is satisfied that provision of those services has not compromised the auditor's independence;

(H) assessment of the performance and objectivity of the Company's internal audit function;

(I) review of the Company's risk management and internal control systems; and

(J) recommendations for the appointment, or if necessary, the dismissal of the head of internal audit;

(ii) provide an open avenue of communication between internal audit, the external auditors and the Board. For the purpose of supporting the independence of their function, the external auditor and the internal auditor (if one is appointed) will have a direct line of reporting access to the Committee;

(iii) review any other reports the Company issues that relate to Committee responsibilities;

(h) **Related party transactions**

(i) review, monitor and approve related party transactions and investments involving the Company and its directors and/or officers, to the extent required under the Companies Law and other rules;

(ii) review and approve all transactions in which the Company is a participant and in which any parties related to the Company (including its executive officers, Directors, beneficial owners of more than 5% (substantial holding) of the

Company's shares, immediate family members of the foregoing persons and any other persons whom the Board determines may be considered related parties of the Company) has or will have a direct or indirect material interest;

(iii) the Committee should only approve those related party transactions that are determined to be in, or are not inconsistent with, the best interests of the Company and its shareholders, after taking into account all available facts and circumstances as the Committee or the Chair of the Company determines in good faith to be necessary. Transactions with related parties or shareholders who have voting power in at least 10% of the Company may also be subject to shareholder approval to the extent required by the ASX Listing Rules;

(i) **Other responsibilities**

(i) review the adequacy of external reporting by the Company to meet the needs of shareholders;

(ii) review the adequacy of the Company's and its subsidiaries insurance policies;

(iii) perform other activities related to this Charter as requested by the Board including where requested by the Board, evaluate, approve and monitor major capital expenditure, capital management and all major acquisitions, divestitures and other corporate transactions, including the issue of securities of the Company;

(iv) institute and oversee special investigations as needed;

(v) confirm annually that all responsibilities outlined in this Charter have been carried out;

(vi) evaluate the Committee's and individual members' performance on a regular basis;

(vii) establish and maintaining free and open means of communication between the Committee, the Company's internal auditor, the Company's internal audit/financial control department and management with respect to auditing and financial control matters, including providing such parties with appropriate opportunities to meet privately with the Committee; and

(viii) perform such additional activities and consider such other matters within the scope of its responsibilities or duties according to applicable law and/or as the Committee and/or the Board deems necessary or appropriate.

6 Review of Committee and Committee Charter

6.1 The Committee will review annually its activities and the manner in which it has carried out its responsibilities, and report to the Board on the outcome of the review.

6.2 The Committee will review annually the terms of the Charter. The Committee may recommend to the Board any changes to this Charter. Any amendments to this Charter must be approved by the Board.

7 Compensation

7.1 Members of the Committee may receive compensation for their service as Committee members, subject to the provisions of the Companies Law and the ASX Listing Rules.

7.2 Members of the Committee may not receive any compensation from the Company except the fees that they receive for service as members of the Board or any committee thereof.

8 Delegation of Authority

Subject to the provisions of the Companies Law, the Committee may delegate to one or more designated members of the Committee the authority to pre-approve audit and permissible non-audit services, provided such pre-approval decision is presented to the full Committee at its scheduled meetings.

Schedule 4

Remuneration and Nomination Committee Charter

Way 2 Vat Limited

(Company)

1 Objectives

The Remuneration and Nomination Committee (**Committee**) is a committee established by the board of directors (**Board**) of the Company. The objectives of the Committee are to:

(a) review and advise the Board on the composition of the Board and its committees;

(b) advise on the process of recruitment, appointment and re-election of directors;

(c) review the performance of the Board, the Chairperson, the executive and non-executive directors and other individual members of the Board;

(d) ensure proper succession plans are in place for consideration by the Board;

(e) assist the Board with the establishment of remuneration policies and practices for the Company's Chief Executive Officer, senior managers and staff, as well as to ensure director compensation is fair and current;

(f) evaluate the competencies required of prospective directors (both non-executive and executive) identify those prospective directors and establish their degree of independence; and

(g) make recommendations to the Board and shareholders accordingly.

2 Authority

2.1 The Committee has authority to conduct or authorise investigations into any matters within its scope of responsibility, to undertake the specific duties and responsibilities listed below and such other specific duties as the Board from time to time prescribes, subject to the limitations of Section 112 of the Israeli Companies Law, 1999 (**Companies Law**). It is authorised to:

(a) retain outside counsel, accountants or other experts, at the expense of the Company, to advise the Committee or assist in the conduct of any matter;

(b) seek any information it requires from employees (all of whom are directed to cooperate with the Committee's requests) or external parties; and

(c) meet with Company officers, employees, external auditor, internal auditor (if any) or outside counsel, as necessary and without management present.

2.2 The Committee will make recommendations to the Board on all matters requiring a decision from the Board. The Committee does not have the power or authority to make a decision in the Board's name or on its behalf.

2.3 The Committee may, in its sole discretion, retain or obtain the advice of a compensation consultant, legal counsel or other adviser and shall be directly responsible for the appointment, compensation and oversight of the work of any compensation consultant, legal counsel and other adviser retained by the Committee. The Committee shall have sole authority to approve the payment of reasonable compensation to a compensation consultant, legal counsel or other adviser retained by the Committee, and other retention terms.

2.4 The Committee may form and delegate authority to subcommittees when appropriate and subject to the Companies Law.

3 Membership

3.1 Members of the Committee shall comprise members of the Board appointed by the Board.

3.2 The number of members of the Committee shall be a minimum of three directors, all of the external directors as defined under the Companies Law shall be members and other members shall be appointed in compliance with Section 244 of the Companies Law. The Board will annually appoint the members of the Committee and nominate the Chair of the Committee, as soon as practical after the Company's annual meeting of shareholders. The Committee Chair will be an independent director who is not Chair of the Board.

4 Committee Meetings

4.1 Meetings shall be held as required but not less than twice per year having regard to the occurrence of Board vacancies and when director and executive remuneration is due for review. Any member of the Committee may request a meeting at any time if they consider it necessary and the Committee may establish its own schedule, which it will provide to the Board in advance. At least once a year the Committee will consider equity compensation plans, performance goals and incentive awards, and the overall coverage and composition of the compensation package to the Company's executive officers.

4.2 A quorum of the Committee will comprise of a majority of the Committee members. However, all members of the Committee are expected to attend and participate in Committee meetings.

4.3 A member of the Committee must not be present for discussions at a Committee meeting on, or vote on a matter regarding, his or her remuneration, election, re-election, or removal.

4.4 If the Committee Chair is absent from a meeting and no acting chair has been appointed, the Committee members present may choose one of them to act as chair for that meeting. A separate chair will be appointed if and when the Committee is dealing with the appointment of a successor to the Committee Chair.

4.5 Non-Committee members may be invited by the Committee Chair to attend meetings of the Committee.

4.6 Reasonable notice of meetings and the business to be conducted shall be given to the members of the Committee and any other person invited by the Committee to attend.

4.7 Meetings of the Committee may be held or participated in by conference call or similar means, and decisions may be made by circular or written resolution.

4.8 Each member of the Committee will have one vote. The action of a majority of those present at a meeting, at which a quorum is present, shall be the act of the Committee.

4.9 The Committee Chair will not have a casting vote. If there is a tied vote, the motion will lapse.

4.10 Following each meeting, the Committee Chair will report to the Board on any matter that should be brought to the Board's attention and on any recommendation of the Committee that requires Board approval or action, and provide the Board with sufficient information upon which to make a decision in that regard.

4.11 Minutes of meetings of the Committee will be prepared for approval by the Committee and be circulated to the members of the Board.

4.12 The Company Secretary will provide such assistance as may be required by the Chairperson in relation to preparation of the agenda, minutes or papers for the Committee.

5 Responsibilities

5.1 The responsibilities of the Committee are to:

(a) **Remuneration**

(i) set and review separately, the policies and practices of the Company regarding the remuneration of non-executive directors and the remuneration of executive directors and other senior management. The Committee may take into account the performance review of senior managers when setting and/or reviewing their remuneration;

(ii) review all components of the remuneration framework of the Chief Executive Officer and such other senior managers as the Board may from time to time determine. The components may include base salary, reimbursable expenses, bonuses, entitlements under employee incentive plans, any equity based remuneration, and all other entitlements and benefits arising from their employment. In reviewing and recommending such matters, the Committee shall consider such matters as it deems appropriate, including the Company's financial and operating performance, the alignment of the interests of the executive officers and the Company's shareholders, the performance of the Company's ordinary shares and the Company's ability to attract and retain qualified individuals. The Chief Executive Officer may not be present during voting or deliberations about his or her compensation;

(iii) annually review the remuneration policy and all components of the remuneration of the non-executive directors. Such components shall include base fees, supplemental fees for undertaking additional duties, reimbursable expenses, entitlements on retirement from or termination of Board membership, any equity incentives, the process by which any pool of directors' fees which has been approved by shareholders is allocated to directors, and all other benefits and entitlements arising from their directorships;

(iv) review the terms of employment contracts for the personnel referred to above;

(v) review the terms of any Company short or long-term incentive plans including any share and option schemes for employees and/or directors. The Committee shall act as Administrator (as defined therein) of the Company's equity compensation plans (to the extent allowed by applicable law and the relevant plan) and any subsequent employee benefit plans adopted and approved by the Company's Board and shareholders, if appropriate. In its administration of the plans, the Committee may, pursuant to authority delegated by the Board (i) recommend to the Board the granting of share options, restricted shares or restricted share units or share purchase rights to individuals eligible for such grants, and (ii) amend such share options, restricted shares or restricted share units or share purchase rights. The Committee shall also make recommendations to the Board with respect to amendments to the plans, including changes in the number of shares reserved for issuance thereunder;

(vi) review the terms of the Company's superannuation and/or pension schemes;

(vii) review any gender or other bias in remuneration for directors, senior managers or other employees of the Company;

(viii) review succession plans for the Board, Chief Executive Officer and other senior managers;

(ix) review such other matters relating to remuneration issues as may be referred to it by the Board;

(b) **Nomination**

(i) develop and review a formal transparent process for selection, appointment and re-appointment of directors, subject to Shareholders' approval as per the Companies Law;

(ii) identify and nominate, for the approval of the Board and the Shareholders, candidates to fill Board vacancies as and when they arise, having regard to the desired composition of the Board as stated in the Board Charter;

(iii) evaluate the competencies required of prospective directors (both non-executive and executive) identify those prospective directors and establish their degree of independence;

(iv) regularly review the structure, size and composition (including the skills, knowledge and experience) of the Board in accordance with applicable law and to make recommendations to the Board regarding any changes to ensure a diverse range of candidates are selected and any gaps in the skill or experience of the board are identified;

(v) inform the Board of the names of directors who are retiring in accordance with the provisions of the Company's articles of association and make recommendations to the Board as to whether the Board should support the re-nomination of that retiring director. In order to make these recommendations, the Committee will review the retiring director's performance during the period in which the director has been a member of the Board;

(vi) undertake appropriate checks before appointing a person or putting forward to shareholders a new candidate for election, as a director;

(vii) provide shareholders with all material information in the Committee's possession relevant to a decision on whether or not to elect or re-elect a director of the Company (including biographical details, qualifications, the candidate's independence and a statement from the Board as to whether it supports the candidate's existing directorships (if any));

(viii) establish with each candidate for a non-executive directorship their commitments outside the Company and the time involved with each, and obtain from each a written statement confirming they are able to dedicate sufficient time to the position;

(ix) propose measurable objectives to assist the Company to achieve gender diversity for adoption by the Board, annually review the Company's progress in meeting each objective and report to the Board on the effectiveness of the objectives and the Company's progress;

(x) establish and facilitate an induction program for new directors with all such information and advice which may be considered necessary or desirable for the director to commence their appointment to the Board;

(xi) require non-executive directors to inform both the Chair of the Company and the Chair of the Committee before accepting any new directorships;

(xii) identify any specific responsibilities of individual Board members, including the Company's Chair;

(xiii) critically review the skills, performance, and effectiveness of the Board, its committees, and its individual members;

(xiv) create and maintain a skills matrix setting out the mix of skills and diversity that the Board currently has or is looking to achieve in its membership; and

(xv) such other matters relating to Board nomination or succession issues as may be referred to it by the Board.

5.2 The Committee may make recommendations to the Board in relation to any of the above.

6 Review of the Committee

6.1 The Committee will prepare and provide to the Board annually:

(a) a self-evaluation of its performance against this Charter;

(b) recommended goals and objectives for the coming year; and

(c) recommended changes or improvements to this Charter if necessary.

6.2 The Committee, in order to ensure that it is fulfilling its duties to the Company and its shareholders will periodically:

(a) obtain feedback from the Board on the Committee's performance and implement any agreed actions; and

(b) provide any information the Board may request to facilitate its review of the Committee's performance.

6.3 The Board shall review the performance of the Committee, at least once per year.

7 Reporting Procedures

7.1 After each meeting, the Chairperson will report the Committee's recommendations and findings to the Board.

7.2 The Chairperson will present an annual report to the Board summarising the Committee's activities during the year and any related significant results and findings.

8 Revisions of this Charter

The Committee is responsible for reviewing the effectiveness of this Charter and the operations of the Committee. The Committee may recommend to the Board any changes or improvements to this Charter. Any amendments to this Charter must be approved by the Board.

9 Compensation

Members of the Committee may receive compensation for their service as Committee members, subject to the Companies Law and the Corporations Act.

Schedule 5

Continuous Disclosure Policy

Way 2 Vat Limited

(Company)

1 Scope

This Policy applies to all executive and non-executive directors, officers, employees, contractors and consultants of the Company and its subsidiaries from time to time (**Personnel**).

2 Purpose

2.1 Company has adopted a set of procedures and guidelines in relation to its continuous disclosure obligations under the ASX Listing Rules and the *Corporations Act 2001* (Cth).

2.2 ASX Listing Rule 3.1 details the Company's primary continuous disclosure obligations. The Company must immediately notify ASX of information that a reasonable person would expect to have a material effect on the price or value of the Company's securities when the Company becomes aware of the information (i.e. 'materially price sensitive information'), unless the materially price sensitive information falls within the exemptions in ASX Listing Rule 3.1A. In this context, ASX has confirmed in Guidance Note 8 that 'immediately' means 'promptly and without delay.'

2.3 The Company is committed to taking a proactive approach to continuous disclosure and creating a culture within the Company that promotes and facilitates compliance with the Company's continuous disclosure obligations.

3 Responsibilities of the Board

3.1 The Company's board of directors (**Board**) bears the primary responsibility for the Company's compliance with its continuous disclosure obligations and is therefore responsible for overseeing and implementing this Policy. The Board makes the ultimate decision on whether there is any materially price sensitive information that needs to be disclosed to the ASX. It is a standing agenda item at all Board meetings to consider any information that must be disclosed to the ASX in accordance with the Company's continuous disclosure obligations.

3.2 The Company has appointed the Company Secretary as the Reporting Officer in order to streamline the day-to-day compliance with its continuous disclosure obligations. All directors are required to notify the Reporting Officer if they believe there is materially price sensitive information which requires disclosure to the ASX. All directors are encouraged to approach the Reporting Officer if they have any queries about what information should be disclosed to the ASX.

4 Responsibilities of the Company Secretary

The Company has appointed the Company Secretary as its ASX liaison officer, being the person responsible for communicating with ASX with respect to all Listing Rule matters. The Company Secretary plays an important role in the Company's continuous disclosure compliance program and is responsible for:

(a) maintaining, and monitoring compliance with this Policy;

(b) liaising between themselves, the Board and the ASX;

(c) overseeing and coordinating disclosure of information to the ASX, analysts, brokers, shareholders, the media, and the public;

(d) coordinating education within the Company about its continuous disclosure obligations and disclosure compliance program;

(e) review information obtained through the Company's reporting systems to determine whether the information is materially price sensitive information; and

(f) coordinating the timely dispatch to the Board of all material market announcements promptly after they have been made; and

(g) providing reports to the board on the effectiveness of the continuous disclosure program.

5 Responsibilities of the Authorised Company Spokesperson(s)

5.1 The Company has appointed the Chairperson and Chief Executive Officer, or in their absence their delegate, as authorised spokespersons. The above people are authorised to make any public statement on behalf of or in relation to the Company following approval of such statements by the Board. Such public statements extend to all responses by the Company to enquiries by the media, analysts or shareholders. All enquiries by regulators should be passed on to the Chief Executive Officer.

5.2 There must be no selective disclosure of materially price sensitive information. The spokesperson should not disclose any materially price sensitive information through public statements which has not already been released to the market through the ASX, but may clarify materially price sensitive information which has already been disclosed to the ASX. Prior to making any public statement, the spokesperson should liaise with the Company Secretary regarding the Company's disclosure history to avoid the inadvertent release of materially price sensitive information.

5.3 The Company may authorise other persons from time to time to make public statements in particular circumstances.

5.4 In the event of inadvertent selective disclosure of previously undisclosed materially price sensitive information, the person or persons involved should immediately contact the Company Secretary. The Board will determine as soon as practicable whether there is a need (based on who received the unintentional selective disclosure and the probability of dissemination) to disclose the materially price sensitive information to ASX, or to require that the party to whom the materially price sensitive information was disclosed enter into a written confidentiality agreement.

6 Responsibilities of Personnel

All Personnel are required to comply with this Policy and the Company's continuous disclosure obligations.

7 Reporting Obligations

7.1 **Information to be reported**

(a) Subject to the exemption in ASX Listing Rule 3.1A, the Company will notify the ASX as soon as it becomes aware of any information that a reasonable person would expect to have a material effect on the price or value of the Company's securities and make all required securities exchange filings. Examples of types of information that could be materially price sensitive information include:

(i) material acquisitions or divestitures;

(ii) transactions that will lead to a significant change in the nature or scale of the Company's activities;

(iii) a material change in the Company's financial forecast or expected results;

(iv) declaration of a dividend;

(v) entry into, variation or termination of material agreements, including financing arrangements;

(vi) events triggering material accelerations of, or increases in, financial obligations;

(vii) a material change in accounting policy adopted by the Company;

(viii) a rating applied by a rating agency to the Company or its securities, and any change in such a rating; and

(ix) a significant change in market or regulatory conditions which is likely to have a material effect on the Company's results.

(b) The above examples are indicative only, and are not exhaustive. Where the Reporting Officer is unsure whether information is materially price sensitive information, it should take a conservative view and report it to, or discuss it with, the Board. The Company's legal advisers should be consulted where the materiality of information or the obligation to disclose is unclear.

(c) The Company must not release information that is for release to the market to any person until it has given the information to the ASX and has received acknowledgement that the ASX has released the information to the market.

(d) The Company must release to market any new and substantive investor or analyst presentation ahead of the delivery of the presentation, irrespective of whether the presentation contains material new information required to be disclosed under Listing Rule 3.1. The Company will make the presentation available electronically as soon as it reasonably can.

7.2 **Confidential information**

(a) Certain materially price sensitive information does not need to be disclosed if it falls within the scope of the confidentiality exemption in ASX Listing Rule 3.1A. To fall within the exemption, <u>all of the following conditions must be satisfied</u>:

(i) the information falls within one or more the following categories:

(A) it would be a breach of the law to disclose the information;

(B) the information concerns an incomplete proposal or negotiation;

(C) the information comprises matters of supposition or is insufficiently definite to warrant disclosure;

(D) the information is generated for internal management purposes of the Company; or

(E) the information is a trade secret; and

(ii) the information is confidential and ASX has not formed the view that the information has ceased to be confidential; and

(iii) a reasonable person would not expect the information to be disclosed.

(b) Once the Reporting Officer determines that information is materially price sensitive information, the Board will consider the confidentiality of the matter and bears the sole

authority to determine whether a matter should not be disclosed to the ASX on the basis of the confidentiality exemption.

(c) The Reporting Officer should disclose all materially price sensitive information to the Board and should not make a final assessment whether materially price sensitive information should not be disclosed on the basis of the confidentiality exemption in ASX Listing Rule 3.1A. However, to assist the Board in making these decisions, the Reporting Officer should provide details as to why they consider the information may be confidential for the purpose of ASX Listing Rule 3.1A.

(d) The Reporting Officer should take all necessary steps to maintain the confidentiality of all potentially confidential information. For example, potentially confidential information should not be disclosed to external parties except on the basis of a written confidentiality undertaking.

(e) he Company has also put in place a review process which includes verification testing of content and a review and sign-off by management prior to the Board formally approving the release of any public information.

(f) ASX Listing Rule 3.1B provides that if the ASX considers that there is, or is likely to be a false market in the Company's securities, and requests information from the Company to correct or prevent the false market, the Company must give the ASX the information needed to correct or prevent the false market (ie. a false market may cause the exemption to be lost).

7.3 **Reporting obligations of the Reporting Officer**

(a) The Reporting Officer has the following reporting obligations in relation to information that potentially requires disclosure:

(i) immediately report all potentially materially price sensitive information to the Board, either in writing or verbally;

(ii) provide sufficient details of all information to allow the Board to form a view as to whether the potentially materially price sensitive information is in fact materially price sensitive and to prepare the appropriate form of disclosure to the ASX, if necessary; and

(iii) state whether the Reporting Officer considers that the information is confidential for the purpose of ASX Listing Rule 3.1A and the reasons for forming that view.

(b) In addition, the Reporting Officer should provide a formal report to the Board at the end of each month which either provides details of unreported potentially materially price sensitive information regarding their area of responsibility or states that the Reporting Officer is unaware of any unreported potentially materially price sensitive information at that time.

7.4 **Dealing with analysts**

(a) The Company must not give analysts or other select groups of market participants any non-public materially price sensitive information at any time, such as during analyst briefings, when responding to analysts' questions or when reviewing draft analyst research reports. The Company may clarify or correct any errors of interpretation that analysts make concerning already publicly available information, but only to the extent that the clarification or correction does not itself amount to giving the analyst non-public materially price sensitive information (such as correcting market expectations about profit forecasts). Any non-public materially price sensitive information that may be inadvertently disclosed during dealings with analysts should be immediately disclosed to the ASX.

(b) All information given to analysts at a briefing, such as presentation slides, and any presentation material from public speeches given by Board members or members of

management that relate to the Company or its business should also be given to the Company Secretary for immediate release to the ASX and posted on the Company's website. The information must always be released to the ASX before it is presented at an analyst or investor briefing.

7.5 **Review of analyst reports**

(a) If requested, the Company may review analyst reports. The Company's policy is that it only reviews these reports to clarify historical information and correct factual inaccuracies (provided this can be achieved using information that has been disclosed to the market generally).

(b) No comment or feedback will be provided on financial forecasts, including profit forecasts prepared by the analyst, or on conclusions or recommendations detailed in the report. The Company communicates this policy whenever asked to review an analyst report.

7.6 **Market speculation and rumours**

(a) In general, the Company does not respond to market speculation and rumours except where:

(i) the speculation or rumours indicate that the subject matter is no longer confidential and therefore the exception to disclosure in the ASX Listing Rules no longer applies;

(ii) the ASX formally requests disclosure by the Company on the matter (under ASX Listing Rule 3.1B); or

(iii) the Board considers that it is appropriate to make a disclosure in the circumstances.

(b) Only authorised spokespersons may make statements on behalf of the Company in relation to market rumours or speculation. Any person within the Company should report market speculation or rumours to the Company Secretary immediately.

7.7 **Trading halts**

(a) It may be necessary to request a trading halt from the ASX to maintain orderly trading in the Company's securities and to manage disclosure issues. The Board will make all decisions in relation to trading halts. No Company Personnel is authorised to seek a trading halt except with the approval of the Board.

7.8 **Website**

(a) All Company announcements will be posted on the Company's website immediately after they are released to the ASX to provide accessibility to the widest audience.

8 Compliance

Breaches of this Policy will be viewed seriously and may lead to disciplinary action being taken against the relevant Personnel. In serious cases, such action may include dismissal or termination of employment or engagement with the Company. Personnel should report all breaches of this Policy by any person to the Company Secretary.

9 Review of the Policy

This Policy will be reviewed regularly by the Board having regard to the changing circumstances of the Company and any changes to this Policy will be notified to affected persons in writing. Personnel should communicate all comments and concerns about this Policy to the Company Secretary.

10 Questions

For questions about the operation of this Policy, please contact the Company Secretary.

11 Definitions

In this Policy, the following definitions apply:

ASX means ASX Limited or the Australian Securities Exchange as the context requires;

Reporting Officer means the Company Secretary or other person appointed to this role by the Company from time to time; and

shareholder includes holders of shares, options or other securities of the Company.

Schedule 6

Risk Management Policy

Way 2 Vat Limited

(Company)

1 Purpose

1.1 The Company considers ongoing risk management to be a core component of the management of the Company. The Company's ability to identify and address risk is central to achieving its corporate objectives.

1.2 This Policy outlines the program implemented by the Company to ensure appropriate risk management within its systems and culture.

2 The Risk Management Program

2.1 The Company's risk management program comprises a series of processes, structures and guidelines which assist the Company to identify, assess, monitor and manage its business risk, including any material changes to its risk profile.

2.2 To achieve this, the Company has clearly defined the responsibility and authority of the Board to oversee and manage the risk management program, while conferring responsibility and authority on the Audit and Risk Management Committee to develop and maintain the risk management program in light of the day-to-day needs of the Company. The Audit and Risk Management Committee is governed by the Audit and Risk Management Committee Charter, a copy of which is available on the Company's website.

2.3 Regular communication and review of risk management practice provides the Company with important checks and balances to ensure the efficacy of its risk management program.

2.4 The key elements of the Company's risk management program are detailed below.

3 Risk Identification

3.1 In order to identify and assess material business risks, the Company defines risks and prepares risk profiles in light of its business plans and strategies. This involves applying a disciplined process to risk identification, risk assessment and analysis, risk treatment and monitoring and reporting.

3.2 The Company presently focusses on the following types of material risks:

(a) regulatory and compliance risks;

(b) reputational risks;

(c) risks relating to conduct of business; and

(d) risks relating to intellectual property.

4 Responsibilities of the Board

4.1 The Board acknowledges that it is responsible for the overall system of internal control but recognises that no cost effective internal control system will preclude all errors and irregularities.

4.2 The Board has delegated responsibility for reviewing the risk profile including material business risks and reporting on the operation of the internal control system to the Audit and Risk Management Committee. However, the Audit and Risk Management Committee and management may also refer particular risk management issues to the Board for final consideration and direction.

4.3 The Board will review the effectiveness of the Company's risk management framework and internal control system annually to satisfy itself that it continues to be sound and that the entity is operating within the risk appetite set by the Board.

5 Responsibilities of the Audit and Risk Management Committee

The day-to-day oversight and management of the Company's risk management program has been conferred upon the Audit and Risk Management Committee in accordance with the Audit and Risk Management Committee Charter. The Committee is responsible for ensuring that the Company maintains effective risk management and internal control systems and processes and provides regular reports to the Board on these matters. In addition to the risk management responsibilities in its Charter, the role of the Committee is to:

(a) assist the Board to fulfil its oversight responsibilities for the financial reporting process, the system of internal control relating to all matters affecting the Company's financial performance, the audit process;

(b) develop processes in relation to ensuring understanding and contribution by foreign directors who do not speak the relevant language;

(c) assist the Board in monitoring compliance with laws and regulations;

(d) assist the Board to adopt and apply appropriate ethical standards in relation to the management of the Company and the conduct of its business;

(e) implement, review and supervise the Company's risk management program; and

(f) review the adequacy of the Company's insurance policies.

6 Responsibilities of Management

6.1 The Company's management will be responsible for designing and implementing risk management and internal control systems which identify material risks for the Company and aim to provide the Company with warnings of risks before they escalate. Management must implement the action plans developed to address material business risks across the Company.

6.2 Management should regularly monitor and evaluate the effectiveness of the action plans. In addition, management should promote and monitor the culture of risk management within the Company and compliance with the internal risk control systems and processes. Management should report regularly to the Board regarding the status and effectiveness of the risk management program. Such reporting by Management should include regular exception reporting to the Board as well as to the Audit and Risk Committee regarding instances of control weaknesses or failures resulting in elevated exposure for the Company.

6.3 The Company’s management will be responsible for ensuring and disclosing that there are appropriate processes in place to ensure that directors who do not speak the language in which the board or security meetings are held or key documents are written can understand and contribute to the discussions at those meetings and understands and can discharge their obligations in relation to those documents.

6.4 The Company’s management will be responsible for ensuring that meetings of security holders are held in Australia at a reasonable place and time.

6.5 The Company's management will be responsible for having and disclosing a whistle blower policy and ensuring that the Board and the Risk and Audit Committee is informed of any material incidents reported under that policy. This policy will be made available on the Company's website.

6.6 The Company's management will be responsible for having and disclosing an anti-bribery and corruption policy and along side the Risk and Audit Committee, ensuring that the Board is aware of any material breaches of that policy. This policy will be made available on the Company's website.

7 Review of Risk Management Program

7.1 The Company regularly evaluates the effectiveness of its risk management program to ensure that its internal control systems and processes are monitored and updated on an ongoing basis.

7.2 The division of responsibility between the Board, Audit and Risk Management Committee and management aims to ensure that specific responsibilities for risk management are clearly communicated and understood. The reporting obligations of Audit and Risk Management Committee ensure that the Board is regularly informed of material risk management issues and actions. This is supplemented by the evaluation of the performance of the risk management program.

Schedule 7

Securities Trading Policy

Way 2 Vat Limited

(Company)

1 Scope

1.1 This policy details the Company's policy on dealing by personnel of the Company and its related bodies corporate (**Group**) in:

(a) Securities of the Company (**Company Securities**); and

(b) Securities of other entities.

1.2 This Policy applies to all 'personnel' of the Group, including all directors, officers, employees and contractors.

1.3 If you do not understand any part of this policy, the summary of the law, or how it applies to you, you should raise the matter with the Company Secretary before dealing with any Securities covered by this policy.

2 Purpose

2.1 Under Australian legislation, the insider trading laws operate to prohibit people in possession of non–public price sensitive information from dealing in Securities or passing on the information to other people who may deal in Securities.

2.2 Given the restrictions imposed by law, this policy is relevant to all personnel of the Group and their associates.

2.3 This policy also imposes additional restrictions (described below) on:

(a) all Directors and officers of the Group including the Managing Director;

(b) all persons who report directly to the Chief Executive Officer (Senior Executives);

(c) all employees and contractors of the Group;

(d) other persons identified by the Company from time to time; and

(e) 'associates' of the above persons. For the purposes of this policy your 'associates' include:

(i) your spouse or partner;

(ii) your dependent children;

(iii) any trustee of a trust or other fiduciary arrangement under which you, your spouse or partner or your dependent children, is or may be a beneficiary;

(iv) any company in which you hold (directly or indirectly) a majority of the shares or otherwise control (directly or indirectly); and

(v) any other entity in which you are a director, secretary or executive officer; and

(f) other persons identified by the Company from time to time,

(**Restricted Persons**).

3 Meaning of Securities

For the purposes of this policy Securities means shares, debentures, options to subscribe for new shares and options over existing shares, warrant contracts and other derivatives relating to the shares.

4 Insider Trading Laws

4.1 Prohibition

If you have any inside information (as defined below in clauses 4.3(a) to 4.3(c)) about the Company (or another relevant entity, such as a company with which the Company is considering a transaction) which is not publicly known, it is a criminal offence for you to:

(a) trade in the Company Securities (or Securities of the other relevant entity);

(b) advise or procure another person to trade in the Company Securities (or Securities of the other relevant entity); or

(c) pass on (directly or indirectly) inside information (as defined below in clauses 4.3(a) to 4.3(c))) to someone else (including colleagues, family or friends) knowing (or where you should have reasonably known) that the other person will, or is likely to, use that information to trade in, or procure someone else to trade in, the Company Securities (or Securities of the other relevant entity).

4.2 Consequences of insider trading

This offence, called 'insider trading', can subject you to:

(a) criminal liability including large fines and/or imprisonment;

(b) a civil penalty; and

(c) civil liability, which may include being sued for any loss suffered as a result of illegal trading.

4.3 Inside information

(a) 'Inside information' is information that:

(i) is not generally available; and

(ii) if it were generally available, a reasonable person would expect it to have a material effect on the price or value of Company Securities or on a decision to buy or sell Company Securities.

(b) The financial impact of the information is important, but strategic and other implications can be equally important in determining whether information is inside information. The definition of information is broad enough to include rumours, matters of supposition, intentions of a person (including the Company) and information which is insufficiently definite to warrant disclosure to the public.

(c) Importantly, you need not be an 'insider' to come across inside information. That is, it does not matter how you come to know the inside information (for example, you could learn it in the course of carrying out your responsibilities or in passing in the corridor or in a lift or at a dinner party).

4.4 Insider trading is prohibited at all times

(a) If you possess inside information, you must not buy or sell the Company Securities, advise or get others to do so or pass on the inside information to others. This prohibition applies regardless of how you learn the information.

(b) The prohibition on insider trading applies not only to information concerning the Company Securities. If a person has inside information in relation to Securities of another company, that person must not deal in those Securities.

(c) The insider trading prohibitions apply even when a trade falls within an exclusion to the restrictions on trading detailed in this policy if it is undertaken by, or procured by, someone in possession of inside information at the time of the trade.

5 Confidential Information

Related to the above, personnel also have a duty of confidentiality to the Company. You must not reveal any confidential information concerning the Company, use that information in any way which may injure or cause loss to the Company, or use that confidential information to gain an advantage for yourself.

6 Trading restrictions imposed by this policy

6.1 Additional restrictions

(a) Additional restrictions (described below) on trading the Company Securities apply to Restricted Persons (as defined above). The additional restrictions in this policy do not prohibit Restricted Persons from acquiring the Securities under a Company dividend reinvestment plan or an employee equity plan, if either plan exists (however, the additional restrictions will apply to any subsequent trading of the Company Securities acquired under those plans).

(b) It is important to note that although the additional restrictions do not apply to a Restricted Person's participation in a dividend reinvestment plan or an employee equity plan, a Restricted Person must not make an election to participate or cease participation in a dividend reinvestment plan or employee share plan if they are in possession of 'inside information.'

6.2 Reasons for additional restrictions

Restricted Persons are in positions where it may be assumed that they may come into possession of inside information and, as a result, any trading by Restricted Persons may embarrass or reflect badly on them or on the Company (even if a Restricted Person has no actual inside information at the time). This policy is designed to avoid the possibility that misconceptions, misunderstandings or suspicions might arise due to trading by Restricted Persons in Securities.

6.3 Trading windows

(a) Restricted Persons may, subject to the prior clearance requirements in clauses 6.4(a) to 6.4(d), deal in the Company's Securities as a matter of course (unless there is in existence price sensitive information that has not been disclosed as a result of the Company's reliance on an exception under the Listing Rules of the Australian Securities Exchange (**ASX**)) in the following periods:

(i) 20 business days beginning on the first trading day after the Company's annual results are released to ASX;

(ii) 20 business days beginning on the first trading day after the Company's half year results are released to ASX;

(iii) 20 business beginning on the first trading day after the Company's Annual General Meeting; and

(iv) any other period as the board of directors of the Company may decide.

(b) All other periods are prohibited periods (i.e. when dealing in Company Securities is prohibited), unless otherwise permitted by this policy.

(c) The Board may also impose an ad hoc prohibited period during a trading window specified above.

6.4 **Clearance procedures**

(a) If a Restricted Person proposes to deal in the Company's Securities at any time, they must first:

(i) obtain prior written clearance to deal in the Company's Securities from the relevant authorising officer noted in the table below (**Authorising Officer**); and/or

(ii) provide prior written notice of their intention to deal in Company Securities to the relevant person noted in the table below; and

(iii) 23.3 provide confirmation to the relevant person(s) noted in the table below that they are not in possession of 'inside information',

at least two trading days before the proposed dealing.

Restricted Person	Authorising Officer	Prior notification to the Company Secretary and Board
Chair of the Board	Chair of the Risk and Audit Committee	Yes
Other Directors (including Chief Executive Officer)	Chair of the Board	Yes
Senior Executives, and other persons identified by the Company from time to time	Managing Director	Yes
Employees	Not applicable - authorisation no required (notification only)	Yes

(b) If granted, trading consent is only valid for a period of five trading days after notification of approval, or such other period notified by the Authorising Officer to the Restricted Person. Trading consent is automatically deemed to be withdrawn if the person becomes aware of inside information prior to trading.

(c) Any approval to trade can be given, withdrawn or refused by the Company in its discretion without giving any reasons. A decision to refuse approval is final and binding on the person seeking the approval. If approval to trade Company Securities is refused, the person seeking the approval must keep that information confidential and not disclose it to anyone. Any approval to trade under this policy is not an endorsement from the Company and the person doing the trade is individually responsible for their investment decisions and their compliance with insider trading laws.

(d) The insider trading prohibitions apply even when a trade is permitted under this clause if it is undertaken by, or procured by, someone in possession of inside information at the time of the trade.

6.5 **Requirements after trading**

Once a Restricted Person has completed a trade in the Company Securities, the Authorising Officer described in clauses 6.4(a) to 6.4(d), must be:

(a) advised that the trade has been completed and attach the trade confirmation (which may occur via email); and

(b) in the case of Directors, provided with sufficient information to enable the Company to comply with its ASX reporting obligations (including date, price, volume and whether the change occurred during a period outside a trading window and if so, whether written clearance was provided). This information must be provided to ASX as soon as reasonably practicable and in any event no later than three business days after the date of the change.

6.6 **No speculative short term trading**

Restricted Persons should not trade in the Company's Securities on a short term basis or for speculative trading gain.

6.7 **No hedging**

(a) A Restricted Person must not, without prior written approval by the Authorising Officer specified in clauses 6.4(a) to 6.4(d), engage in hedging arrangements, deal in derivatives or enter into other arrangements which vary economic risk related to the Company's Securities including, for example, dealing in warrants, equity swaps, put and call options, contracts for difference and other contracts intended to secure a profit or avoid a loss based on fluctuations in the price of the Company's Securities.

(b) This provision includes engaging in hedging or other arrangements that would have the effect of limiting the economic risk in connection with Company Securities including Securities which are unvested, subject to a holding lock or issued pursuant to an equity based remuneration scheme.

6.8 **Permitted dealings**

Certain types of dealing are excluded from the operation of this policy and may be undertaken at any time (subject to complying with the insider trading prohibitions outlined above in clause 4), including the following (and any other permitted dealings as approved by the Board from time to time and notified to Restricted Persons):

(a) employee incentive schemes – the additional restrictions in this policy do not prohibit Restricted Persons from acquiring Securities or exercising an option or right under an employee incentive scheme subject to the terms of the relevant employee incentive scheme. However, the additional restrictions will apply to any subsequent trading of Securities acquired under an employee incentive scheme and the Restricted Person must make an election to participate or cease participation in an employee incentive scheme when they are not in possession of inside information;

(b) dividend reinvestment plan – the additional restrictions in this policy do not prohibit Restricted Persons from acquiring Securities under a dividend reinvestment plan. However, the additional restrictions will apply to any subsequent trading of Securities acquired under a dividend reinvestment plan and the Restricted Person must make an election to participate or cease participation in a dividend reinvestment plan when they are not in possession of inside information;

(c) rights offers, share purchase plans and buy-backs (or other pro-rata/generalised offers) – trading under an offer or invitation made to all or most of the security holders, such as a rights issue, a security plan purchase and an equal access buy-back, where the plan that determines the timing and structure of the offer has been approved by Board. This includes decisions relating to whether or not to take up the entitlements and the sale of entitlements required to provide for the take up of the balance of entitlements under a renounceable pro rata issue;

(d) third party discretion – an investment in, or trading in units of, a fund or other scheme (other than a scheme only investing in Securities) where the assets of the fund or other scheme are invested at the discretion of a third party; and

(e) disposal under margin lending arrangement – an involuntary disposal of securities that results from a margin lender or financier exercising its rights under a margin lending or other secured financing arrangement that has previously been approved in accordance with this policy.

6.9 **Exceptional circumstances**

(a) If a Restricted Person needs to deal in the Company's Securities due to exceptional circumstances but such dealing would breach this policy, the Restricted Person must apply to the Authorising Officer specified in clauses 6.4(a) to 6.4(d) for a waiver from compliance with the provisions in clauses 6.4(a) to 6.4(d) or 0.

(b) Exceptional circumstances include severe financial hardship, compulsion by a court order or any other circumstances that are deemed exceptional by the person described in clauses 6.4(a) to 6.4(d).

(c) The Restricted Person seeking a waiver under this clause must apply in writing (which may include an application via email) to the person specified in clauses 6.4(a) to 6.4(d):

(i) setting out the circumstances of the proposed dealing (including an explanation as to the severe financial hardship or circumstances that are otherwise exceptional) and the reason the waiver is requested; and

(ii) provide confirmation to the relevant person(s) that they are not in possession of 'inside information'.

(d) A waiver will only be granted if the Restricted Person's application is accompanied by sufficient evidence (in the opinion of the person specified in clauses 6.4(a) to 6.4(d)) that the dealing of the relevant Securities is the most reasonable course of action available in the circumstances.

(e) If a waiver is granted, the Restricted Person will be notified in writing (which may include notification via email) and in each circumstance the duration of the waiver to deal in Securities will be five trading days or such other period notified by the Authorising Officer to the Restricted Person.

(f) Unless otherwise specified in the notice, any dealing permitted under this clause must comply with the other clauses of this policy (to the extent applicable). The insider trading prohibitions apply even when a trade falls within this clause 6.9(f) if it is undertaken by, or procured by, someone in possession of inside information at the time of the trade.

7 Breaches of this policy

Strict compliance with this policy is a condition of employment or engagement by the Company. Breaches of this policy will be regarded as serious misconduct and may lead to disciplinary action, which may include termination of employment or engagement by the Company.

8 Business Unit policies

8.1 Dealing in Securities or communicating information may also be subject to Business Unit policies relating to personal dealing, insider trading, conflicts of interest or similar.

8.2 You must also comply with the requirements of those policies in addition to the requirements in this policy. Please contact Risk and Compliance for further information.

9 Further Information

For more information about this policy, contact the Company Secretary.

Schedule 8

Diversity Policy

Way 2 Vat Limited

(Company)

1 Scope

This diversity policy applies to the Company's board of directors (**Board**), officers and employees (**Personnel**).

2 Purpose

2.1 The Company has a strong commitment to diversity and recognises the value of attracting and retaining Personnel with different backgrounds, knowledge, experiences and abilities. The Company recognises that diversity not only encompasses gender but extends to age, ethnicity, religious or cultural background, language, marital or family status, and disability. Diversity contributes to the Company's business success and benefits individuals, clients, teams, shareholders and stakeholders.

2.2 Our business policies, practices and behaviours promote diversity and equal opportunity and create an environment where individual differences are valued and all Personnel have the opportunity to realise their potential and contribute to the Company's success.

3 What is Diversity?

3.1 Diversity recognises and values the contribution of people with differences in background, experience and perspectives. At the Company, diversity means:

(a) an inclusive workplace that embraces individual differences;

(b) a workplace that is free from discriminatory behaviours and business practices including discrimination, harassment, bullying, victimisation and vilification;

(c) equitable frameworks and policies, processes and practices that limit potential unconscious bias;

(d) equal employment opportunities based on capability and performance;

(e) awareness of the different needs of employees;

(f) the provision of flexible work practices and policies to support employees; and

(g) attraction and retention of a diverse range of talented people.

3.2 The Company aspires to achieve the objectives in this policy and aims to embed a strong diversity framework within its systems and culture.

4 Board's Responsibilities

4.1 The Board is responsible for designing and overseeing the implementation of this diversity policy.

4.2 The directors of the Company will be responsible for promoting diversity within the Company's culture and monitoring the effectiveness of this diversity policy. The Company recognises that it needs to provide management with appropriate guidance in order to foster a value for

diversity within its management culture. To achieve this, the Company is committed to providing its management with the appropriate training and resources to understand the benefits of diversity in recruitment strategies and day-to-day management strategies. The Board will also be required to develop initiatives that will promote and achieve diversity goals.

4.3 The Board will disclose at the end of each reporting period the measurable objectives for achieving gender diversity as set by the Board and the Remuneration and Nomination Committee in accordance with the diversity policy.

4.4 The Company will make the policy or a summary of it available on its website.

5 Remuneration and Nomination Committee's Responsibilities

The Remuneration and Nomination Committee (if any) is responsible for reviewing this diversity policy and will provide the Board with an annual report on the status of diversity within the Company and the effectiveness of the measurable objectives for achieving gender diversity.

6 Personnel's Responsibilities

All Personnel are required to act in a manner that supports diversity within the workplace and promotes the objectives set out in this diversity policy. Employees are encouraged to provide feedback to management regarding programs or initiatives which will improve the Company's approach to diversity and inclusion in the workplace.

7 Measureable objectives

7.1 The Company recognises that gender diversity amongst its Personnel:

(a) broadens the pool of high-quality directors and employees;

(b) is likely to support employee retention;

(c) is likely to encourage greater innovation by drawing on different perspectives;

(d) is a socially and economically responsible governance practice; and

(e) will improve the Company's corporate reputation.

7.2 Subject to the size and operations of the Company, the Board may adopt measureable objectives to assist the Company to achieve gender diversity and review the Company's progress in meeting these objectives and the effectiveness of these objectives each year.

7.3 The Remuneration and Nomination Committee (if applicable) is responsible for:

(a) recommending such measureable objectives to the Board in light of the Company's general selection policy for Personnel; and

(b) reporting to the Board on the Company's progress towards achieving its measurable objectives each year. This report will include a review of the relative proportions of men and women at all levels in the organisation.

Schedule 9

Shareholder Communications Policy

Way 2 Vat Limited

(Company)

1 Purpose

1.1 The Company is committed to regularly communicating with shareholders in a timely, accessible and clear manner with respect to both procedural matters and major issues affecting the Company. To achieve this, the Company communicates with shareholders through a range of forums and publications.

1.2 The reference to **shareholder** in this Policy includes holders of shares, options and other securities of the Company.

2 Electronic and Written communications

2.1 The Company aims to ensure that its Annual Report provides shareholders with a good understanding of the Company's activities, performance and position for the previous financial year.

2.2 Shareholders can elect to receive an electronic copy or a hard copy of the Annual Report. The Company encourages shareholders to support its commitment to the environment by electing to receive the Annual Report and other communications electronically by registering their email address with the Company's share registry.

2.3 As detailed in its Continuous Disclosure Policy, the Company is committed to complying with, and taking a proactive approach to, its continuous disclosure obligations. This extends to promptly providing all applicable securities regulators (including the ASX), with all necessary information and communications for publication on the ASX website.

2.4 The Company aims to provide shareholders with comprehensive and timely access to Company documents and releases through its website. The Company's website will include:

(a) copies of the Company's articles of association, Board and committee charters and key corporate governance policies;

(b) copies of all material information lodged with the ASX and any other applicable securities regulators and securities exchanges;

(c) copies of all announcements, briefings and speeches made to the market, analysts or the media;

(d) the last three years of press releases or announcements made by the Company;

(e) the last three years of financial data for the Company;

(f) the full text of notices of shareholder meetings and explanatory material;

(g) the Company's Annual Reports for the last three financial years;

(h) the names, photographs and brief biographical information for each of the Company's directors and senior executives;

(i) webcasts (as and when available);

(j) presentations provided to financial analysts; and

(k) advanced notice of all open briefings to institutional investors and analysts, including presentation materials.

2.5 Other information and updates may be provided to shareholders via periodic mail-outs. In addition, the Company allows shareholders to elect to receive email communications where appropriate.

3 Shareholder Participation

3.1 The Company encourages shareholders to submit questions or requests for information directly to the Company via the Company's website at https://way2vat.com/.

3.2 The Company's board of directors encourages all shareholders to attend and participate in the Company's annual meeting of shareholders.

3.3 The Company's external auditor will attend the Company's annual meeting and will be available to answer questions from shareholders about the conduct of the audit and preparation of the auditor's report.

4 Share Registry and Contact Details

4.1 Shareholders who wish to update personal or contact information, elect to receive communications electronically, or wish to ask a question related to their shareholding in the Company should contact their broker or the Company's share registry, Automic Registry Services.

4.2 The contact details are:

email:	-
telephone:	1300 288 664
post:	Level 5, 126 Phillip Street Sydney NSW 2000
website:	https://www.automicgroup.com.au/

Schedule 10

Whistleblower Policy

Way 2 Vat Limited

(Company)

1 Introduction and purpose

1.1 This Whistleblower Policy (**Policy**) reflects the commitment of Way 2 Vat Limited and each of its subsidiaries (**Company**) to maintain the highest standard of ethical conduct in its activities and ensure appropriate risk management.

1.2 The objects of this Policy are to:

(a) encourage the reporting of suspected or actual wrongdoing;

(b) protect and support the dignity, wellbeing, career and good name of disclosing persons who report suspected or actual wrongdoing;

(c) help deter wrongdoing and support and enhance the Company's long-term sustainability and reputation;

(d) support the Company's values and develop a culture of accountability and continuous improvement;

(e) outline how disclosures will be dealt with and ensure that disclosures are dealt with appropriately and on a timely basis; and

(f) comply with the whistleblowing provisions contained in Part 9.4AAA of the *Corporations Act 2001* (Cth) (**Corporations Act**).

2 Scope and application

2.1 This Policy is available to and applies to all officers and employees of the Company and also to any other persons who are Eligible Whistleblowers.

2.2 This Policy is to be read subject to the Corporations Act and to the extent that the terms of this Policy are inconsistent with the Corporations Act, the terms of the later prevail. Any obligations on the Company under this Policy do not constitute contractual terms.

3 What wrongdoing can be reported?

3.1 While any person can choose to make a disclosure, this Policy addresses the disclosures that will be a protected disclosure under the Corporations Act (ie, a Protected Disclosure). This Policy is not directed at general grievances to the extent that they are not protected under the Corporations Act.

3.2 **Disclosable Matters**

(a) **Disclosable Matters** involve information that the discloser has reasonable grounds to suspect concerns misconduct or an improper state of affairs or circumstances in relation to the Company or a related body corporate of the Company.

(b) Without limitation, Disclosable Matters can involve information that indicates that the Company, one of its related bodies corporate or an officer or employee of the Company or one of its related body corporates has engaged in conduct that:

(i) constitutes an offence against, or a contravention of the Corporations Act, the Australian Securities and Investments Commission Act 2001 (Cth), the Banking Act 1959 (Cth), the Financial Sector (Collection of Data) Act 2001 (Cth), the Insurance Act 1973 (Cth), the National Consumer Credit Protection Act 2009 (Cth), the Superannuation Industry (Supervision) Act 1993 (Cth), or any instrument under any one of these laws;

(ii) constitutes an offence against any other federal law that is punishable by imprisonment for 12 months or more;

(iii) represents a danger to the public or to the financial system; or

(iv) is prescribed by regulation.

(c) Disclosable Matters include matters that may not necessarily involve unlawful conduct or a contravention of a particular law. However, common examples of Disclosable Matters include actual or suspected:

(i) fraud, money laundering, financial irregularities or misappropriation of funds;

(ii) failure(s) to comply with legal or regulatory requirements;

(iii) illegal conduct, such as theft, bribery, dealing in or use of illicit drugs and other criminal activities; and

(iv) detrimental conduct or threatened detrimental conduct against a person who has made a disclosure or is believed or suspected to have made, or be planning to make, a disclosure.

(d) A discloser can still qualify for protection even if their disclosure turns out to be misplaced or incorrect. However, disclosers must not knowingly make a false disclosure.

(e) Disclosures that are not about Disclosable Matters generally do not qualify for protection under the Corporations Act. Such disclosures however may be protected under other legislation, such as the *Fair Work Act 2009* (Cth).

4 Personal work-related grievances

4.1 Disclosures that relate solely to 'personal work-related grievances', and that do not otherwise relate to detriment or threat of detriment to the discloser, ordinarily do not qualify for protection under the Corporations Act (other than where disclosure is made to a legal practitioner for the purposes of obtaining legal advice or legal representation in relation to the operation of the whistleblower provisions in the Corporations Act).

4.2 'Personal work-related grievances' are those that relate to the discloser’s current or former employment and which have, or tend to have, implications for the discloser personally but:

(a) do not have any significant implications for the Company (or another regulated entity); and

(b) do not relate to any conduct, or alleged conduct, about certain disclosable matters.

(c) Examples of 'personal work-related grievances' include:

(d) a grievance as a result of an interpersonal conflict between an employee and another employee;

(e) dissatisfaction with a decision about the engagement, transfer, promotion or terms and conditions of engagement of an employee; or

(f) dissatisfaction with a decision to undertake performance management or disciplinary action in respect of an employee, or otherwise terminate the engagement of the employee.

(g) However, the disclosure of a 'personal work-related grievance' may still qualify for protection under the Corporations Act if:

(h) it includes information about a Disclosable Matter, or information about a Disclosable Matter includes or is accompanied by a personal work-related grievance (ie, it is a mixed report); or

(i) it concerns an allegation that the discloser has suffered, or is threatened with, detriment for making a Protected Disclosure.

4.3 Any personal work-related grievances which are not Protected Disclosures covered by this Policy can be appropriately addressed in consultation with a person's line manager or in accordance with the Company's grievance policy.

5 How can a person disclose suspected wrongdoing?

5.1 **Generally**

(a) To assist the Company identify and address wrongdoing, it is expected that any Eligible Whistleblower who becomes of aware of a Discloseable Matter will make a report.

(b) Where appropriate, persons are encouraged to raise matters of concern informally and outside of this Policy with their line manager or the Company's Human Resources team in the first instance.

(c) Alternatively to an informal report, a person may be entitled to make a Protected Disclosure as set out in this Policy. The making of a Protected Disclosure entitles a discloser to various legal protections (as set out later in this Policy).

5.1 **Disclosure to eligible recipient**

(a) An Eligible Whistleblower can disclose a Disclosable Matter to any of the following persons (eligible recipients):

(i) an officer or Senior Manager of the Company or a related body corporate of the Company, which includes the CEO and CFO of the Company;

(ii) an auditor, or a member of an audit team conducting an audit, of the Company or a related body corporate of the Company;

(iii) an actuary of the Company or related body corporate of the Company;

(iv) a person authorised by the Company to receive disclosures that may qualify for protection under the Corporations Act, including the Whistleblower Protection Officer and any other person who is otherwise authorised by the Company from time-to-time; and

(v) any other person or body prescribed by regulation.

(b) A Disclosable Matter which is disclosed by an Eligible Whistleblower to one of the eligible recipients will be a Protected Disclosure.

5.2 **How do I make a Protected Disclosure to an eligible recipient?**

(a) Without limitation, Protected Disclosures can be made:

(i) in writing, via post or email, to one of the eligible recipients above (any correspondence should be marked 'Strictly confidential – to be opened by addressee only'); and

(ii) to the Whistleblower Protection Officer via email to the Company's whistleblower inbox.

(b) Where a disclosure is received by an eligible recipient who is not the Whistleblower Protection Officer, the disclosure will ordinarily be referred to the Whistleblower Protection Officer for actioning in accordance with this Policy (noting that the discloser's identity must only be disclosed as allowed by this Policy).

(c) If you would like to obtain more information before making a disclosure, including about anything in this Policy, you can contact the Whistleblower Protection Officer or alternatively obtain independent legal advice.

5.3 **Can I remain anonymous?**

(a) A discloser does not have to identify themselves in order to qualify for protection under the Corporations Act. A discloser can choose to remain anonymous while making a disclosure, over the course of an investigation and after an investigation is finalised.

(b) A discloser can refuse to answer questions that they feel could reveal their identity at any time, including during follow-up conversations. However, it is preferred that a discloser who wishes to remain anonymous maintains ongoing two-way communication with the Company, so the Company can ask follow-up questions or provide feedback.

(c) The Company encourages a discloser to share their identity as it may assist the Company to address any matters raised in a Protected Disclosure. Furthermore, the Company may not be able to undertake an investigation if it is not able to contact the discloser (eg, if a disclosure is made anonymously and the discloser has refused to provide, or has not provided, a means of contacting them).

(d) Where a discloser wishes to remain anonymous, communication can occur through anonymised correspondence and a discloser may adopt a pseudonym for the purpose of their disclosure.

6 Other ways to make Protected Disclosures

6.1 The Company encourages its employees and other persons to make an informal disclosure to the Company or a Protected Disclosure to one of the Company's internal eligible recipients in the first instance. However, where appropriate, other disclosures can be made which qualify as Protected Disclosures, including:

(a) disclosures by an Eligible Whistleblower relating to Disclosable Matters made to ASIC, APRA or another Commonwealth authority prescribed by regulation;

(b) disclosures made to a legal practitioner under certain circumstances; and

(c) disclosures made to a journalist or parliamentarian under certain circumstances.

6.2 **Disclosure to legal practitioner**

Disclosures by an individual to a legal practitioner for the purposes of obtaining legal advice or legal representation in relation to the operation of the whistleblower provisions in the Corporations Act qualify for protection under the Corporations Act (even in the event that the legal practitioner concludes that a disclosure does not relate to a Disclosable Matter or the person is not an Eligible Whistleblower).

6.3 **Disclosure to ASIC, APRA or prescribed Commonwealth authority**

An Eligible Whistleblower can make disclosure of information to ASIC, APRA or a prescribed Commonwealth authority and such a disclosure will be a Protected Disclosure if the disclosure involves a Disclosable Matter.

6.4 **Emergency and Public Interest Disclosures**

(a) Disclosures can also be made to a journalist or parliamentarian under certain circumstances and qualify for protection under the Corporations Act. However, a disclosure must have previously been made to ASIC, APRA or a prescribed Commonwealth authority and written notice provided to the body to which the disclosure was made.

(b) The Company encourages employees to make use of the whistleblowing procedures set out in this Policy and internally report matters in the first instance such that it is not necessary to make an Emergency Disclosure or a Public Interest Disclosure to a journalist or parliamentarian.

(c) The Company acknowledges that in some circumstances, it may be necessary for individuals to make such disclosures and that the Company will comply with all legislative requirements, as set out in this Policy, in respect of such disclosures.

6.5 **Emergency Disclosures**

An Emergency Disclosure is a disclosure of information by an individual (the **discloser**) which will be a Protected Disclosure where each of the following criteria are met:

(a) the discloser has previously made a Protected Disclosure to ASIC, APRA or another Commonwealth authority prescribed by regulation (the **previous disclosure**); and

(b) the discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health and safety of one or more persons or to the natural environment; and

(c) before making the Emergency Disclosure, the discloser has given written notification to the body to which the discloser made the previous disclosure which states that the discloser intends to make an emergency disclosure and which includes sufficient information to identify the previous disclosure; and

(d) the Emergency Disclosure is made to a member of parliament (of the Commonwealth or a State or Territory) or a journalist; and

(e) the extent of the information disclosed in the Emergency Disclosure is no greater than necessary to inform the recipient in (d) above of the substantial and imminent danger.

6.6 **Public Interest Disclosures**

A **Public Interest Disclosure** is a disclosure of information by an individual (the **discloser**) which will be a Protected Disclosure where each of the following criteria are met:

(a) the discloser has previously made a Protected Disclosure to ASIC, APRA or another Commonwealth authority prescribed by regulation (the **previous disclosure**); and

(b) at least 90 days have passed since the previous disclosure was made; and

(c) the discloser does not have reasonable grounds to believe that action is being, or has been, taken to address the matters to which the previous disclosure related; and

(d) the discloser has reasonable grounds to believe that making a further disclosure of the information would be in the public interest; and

(e) at least 90 days after the previous disclosure was made and before making the Public Interest Disclosure, the discloser has given written notification to the body to which the

discloser made the previous disclosure which states that the discloser intends to make a Public Interest Disclosure and which includes sufficient information to identify the previous disclosure; and

(f) the Public Interest Disclosure is made to is made to a member of parliament (of the Commonwealth or a State or Territory) or a journalist; and

(g) the extent of the information disclosed in the Public Interest Disclosure is no greater than necessary to inform the recipient in (f) above of the misconduct or the relevant information.

7 Handling and investigation of disclosures

7.1 Receiving a disclosure

(a) Where the Company receives a disclosure through an eligible recipient, it will:

(i) treat the disclosure seriously, confidentially and sensitively;

(ii) acknowledge receipt of the disclosure (provided the Company has a means by which to contact the discloser);

(iii) arrange for the Whistleblowing Protection Officer to conduct a preliminary review of the information disclosed and assess the disclosure to determine whether:

(A) it qualifies for protection and whether a formal, in-depth investigation is required; and

(B) it is of a serious or significant nature; and

(iv) if necessary, the Whistleblowing Protection Officer will arrange for the disclosure to be investigated in accordance with this Policy.

(b) If the matter is of a serious or significant nature, the Whistleblower Protection Officer must, subject to confidentiality restrictions, immediately notify the CEO of the Company or, if the matter involves the CEO of the Company, the Chair of the Board of the Company / next most senior management executive of the Company who is not involved in the matter.

7.2 Investigating a disclosure

(a) The purpose of an investigation is to determine whether there is enough evidence to substantiate or refute the matters reported in a disclosure and consider appropriate further action if necessary.

(b) If the Company determines that an investigation is required, the Company will ordinarily an investigate a disclosure by:

(i) if necessary or possible, contacting the discloser to obtain further information which may be reasonably required to undertake an investigation;

(ii) determining the nature and scope of the investigation and whether any technical, financial or legal advice may be required to support the investigation;

(iii) appointing an appropriately qualified internal or external investigator, which may be the Whistleblowing Protection Officer;

(iv) considering whether any urgent intermediate steps are required to be taken to protect persons or property;

(v) interviewing any relevant witnesses and obtaining relevant documentary evidence;

(vi) objectively considering evidentiary material to determine whether there is evidence of misconduct or an improper state of affairs or circumstances established;

(vii) preparing a confidential investigation report and reporting the outcome of the investigation to senior management and any regulatory bodies as required by law; and

(viii) if necessary, consulting with internal or external legal counsel to determine how the Company will respond and/or report the matter.

(c) The above processes and timeframe may vary depending on the nature of the disclosure. Throughout an investigation, the investigator must remain objective and, to the extent possible, accord procedural fairness to all persons who may be involved in the investigation.

(d) The Company will endeavour to conduct and conclude all investigations within one month of the disclosure being received.

(e) If limited information is received from a discloser, the Company may investigate a disclosure to the extent possible, such as by conducting a broad review of the subject matter or the work area disclosed.

(f) All officers and employees of the Company are required to cooperate fully with any investigations conducted under this Policy.

7.3 **Reporting of outcomes**

(a) The Company's method for documenting and reporting the findings will depend on the nature of the disclosure.

(b) A discloser will usually be provided with regular updates, if the discloser can be contacted (including through anonymous channels). The frequency and timeframe of updates may vary depending on the nature of the disclosure, however the Company will endeavour to ensure a discloser is kept updated in relation to the next steps and advised of when any investigation is commenced or completed.

(c) Ordinarily at the conclusion of an investigation, a discloser will receive a written communication which advises the outcome of the investigation, including findings as to whether any concerns have been substantiated and summarises the evidence on which the findings are based. There may, however, also be circumstances where it may not be appropriate or possible to provide details of the outcome to the discloser.

(d) At the conclusion of an investigation, the investigator must submit a written report to the CEO of the Company (or the Chair of the Board of the Company if the investigation involves the CEO). The process and findings of an investigation must be documented and included in the report to the CEO (or the Chair of the Board of the Company if the investigation involves the CEO), while protecting the identity of the discloser (unless the discloser has otherwise consented to the disclosure of their identity).

(e) Where an investigation of a disclosure establishes a breach of the Company's policies, appropriate disciplinary action may be taken against those persons involved in the disclosed circumstances.

7.4 **Keeping of records**

The Company must ensure appropriate records and documentation for each step in the process are maintained and securely kept for 7 years. This includes an notes and evidentiary material collected or considered during the course of the investigation.

7.5 **Handling of personal information**

Any personal information provided to the Company by a discloser will be treated in accordance with the Company's Privacy Policy and the Corporations Act.

8 Treatment of employees mentioned in disclosures

8.1 Where Company employees are mentioned in, or are related to a matter about which a discloser has made a Protected Disclosure, the Company will take reasonable steps to ensure fair treatment of those named employees. This may include:

(a) keeping the matter of the disclosure as confidential as possible;

(b) ensuring each disclosure will be assessed and, where appropriate, formally investigated;

(c) informing Company investigators, managers and officers only on a need-to-know basis;

(d) when an investigation needs to be undertaken, ensuring the process is objective, fair and independent;

(e) ensuring an employee who is the subject of a disclosure is advised about the subject matter of the disclosure as and when required by principles of procedural fairness;

(f) directing other employees or officers to take, or abstain from, particular actions;

(g) not taking any form of disciplinary action unless and until findings are made; and

(h) making counselling and support services available through the Company's EAP provider.

8.2 The Company will not tolerate the ill treatment, including victimisation or bullying, of any officer or employee mentioned in, or related to, a disclosure of the kind protected under this Policy. Any such ill treatment may result in disciplinary action being taken, up to and including summary termination of employment.

9 Protections for disclosers

9.1 The Company is committed to providing support and protection in response to genuine reports of wrongdoing and will not tolerate reprisals or threats of reprisals against a discloser who has made a Protected Disclosure.

9.2 The Company prohibits the ill treatment, including victimisation or bullying, of any Company employee who makes a Protected Disclosure. Any such ill treatment may result in disciplinary action being taken, up to and including summary termination of employment.

9.3 In addition to the Company's policies against victimisation, legal protections are available to disclosers who qualify for protection under Part 9.4AAA of the Corporations Act. These protections include:

(a) identity protection (confidentiality);

(b) protection from detrimental acts or omissions;

(c) compensation and other remedies; and

(d) civil, criminal and administrative liability protection.

9.1 **Identity protection and confidentiality**

(a) It is generally unlawful for a person to disclose the identity of a discloser, or disclose information that is likely to lead to the identification of the discloser, in respect of a Protected Disclosure where the identity or information is information which the person has obtained directly or indirectly because of the Protected Disclosure.

(b) There are exceptions to this prohibition in relation to Protected Disclosures, such that information may be disclosed to:

(i) any person, with the consent of the discloser;

(ii) ASIC, APRA or a member of the Australian Federal Police;

(iii) a legal practitioner, for the purposes of obtaining legal advice or representation in relation to the operation of Part 9.4AAA;

(iv) a Commonwealth authority, or a State or Territory authority, for the purpose of assisting the authority in the performance of its functions or duties; or

(v) a person or body prescribed by regulation.

(c) Furthermore, a person can disclose the information contained in a disclosure with or without the discloser's consent if:

(i) the information does not include the discloser's identity;

(ii) the person has taken all reasonable steps to reduce the risk that the discloser will be identified from the information; and

(iii) it is reasonably necessary for investigating the issues raised in the disclosure.

(d) The identity of a discloser, who has made a Protected Disclosure, may be required to be revealed to a court where it is necessary to give effect to the Corporations Act or where it is in the interests of justice to do so.

(e) All officers and employees of the Company must ensure the identity of a discloser, who has made a Protected Disclosure, remains confidential unless disclosure is allowed or required by law.

(f) In order to protect the confidentiality of a discloser's identity, the Company will ensure that:

(i) access to all information relating to a disclosure will be limited to those directly involved in managing and investigating the disclosure;

(ii) disclosures will be handled and investigated by appropriately trained and qualified persons;

(iii) each person who is involved in handling and investigating a disclosure will be reminded about the confidentiality requirements, including that an unauthorised disclosure of a discloser's identity may be a criminal offence;

(iv) communications, documents and records relating to a disclosure or an investigation of a disclosure will be securely stored and will not be accessible by other staff;

(v) where possible, all personal information or reference to the discloser will be redacted and the discloser will be referred to in a gender-neutral context; and

(vi) the consent of discloser is obtained prior to their identity or identifying information being disclosed to other persons.

9.2 **Protection from detrimental acts or omissions**

(a) The Company will not tolerate express or implied threats (whether conditional or unconditional) or conduct, that causes any detriment to another person where the person threatening, or carrying out, the conduct does so because they believe or suspect that the other person is, may or has been, a discloser who has or may make a Protected Disclosure.

(b) It is unlawful for a person to engage in conduct that causes detriment to a discloser (or another person), in relation to a disclosure, if:

(i) the person believes or suspects that the discloser (or another person) made, may have made, proposes to make or could make a Protected Disclosure; and

(ii) the belief or suspicion is the reason, or part of the reason, for the conduct.

(c) It is also unlawful for a person (the **first person**) to make a threat (whether express or implied, conditional or unconditional) to cause any detriment to a second person or a third party because a person makes a Protected Disclosure or may make a Protected Disclosure, where the first person:

(i) intends the second person to fear that the threat will be carried out; or

(ii) is reckless as to causing the second person to fear that the threat will be carried out.

(d) However, the following actions are not unlawful detrimental conduct:

(i) administrative action that is reasonable for the purpose of protecting a discloser from detriment (such as relocating a discloser's immediate worker area); and

(ii) managing a discloser’s unsatisfactory work performance, in line with the Company's performance management framework.

(e) To protect disclosers from detrimental acts or omissions, the Company will:

(i) conduct training from time-to-time to ensure that relevant staff are aware of their responsibilities to, amongst other things, not engage in victimisation;

(ii) investigate any complaints made by a discloser of any actual, suspected or threatened of detrimental conduct; and

(iii) consider strategies to help a discloser minimise and manage stress, time or performance impacts, or other challenges resulting from the disclosure or its investigation.

9.3 **Protection from civil, criminal and administrative liability**

(a) A discloser, who has made a Protected Disclosure, is protected under the Corporations Act as follows:

(i) they are protected from any civil, criminal or administrative liability (including disciplinary action) for making the Protected Disclosure;

(ii) no contractual or other remedy may be enforced, and no contractual or other right may be exercised, against the discloser on the basis of their Protected Disclosure; and

(iii) the information they have disclosed is not admissible in evidence against the person in criminal proceedings or in proceedings for the imposition of a penalty, other than proceedings in respect of the falsity of the information, where the disclosure is protected by virtue of being:

(A) an Emergency Disclosure or Public Interest Disclosure; or

(B) a Protected Disclosure to ASIC, APRA or other prescribed Commonwealth authority.

(b) The above protections, however, do not grant immunity to a discloser for any misconduct a discloser has engaged in that is revealed as a result of their disclosure.

9.4 **Compensation and other remedies**

(a) A discloser (or any other employee or person) can seek compensation and other remedies under the Corporations Act through the courts if they suffer loss, damage or injury because of a Protected Disclosure and the Company failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

(b) The Company encourages disclosers to seek their own independent legal advice about their legal rights where necessary.

10 Support for disclosers

10.1 The Company will take appropriate measures to support the health and wellbeing of a discloser making a Protected Disclosure which are tailored to the circumstances of any particular case. This support may be in the form of:

(a) offering the discloser access to counselling and support through the Company's Employee Assistance Program (EAP) provider;

(b) directing other employees or officers to take, or abstain from, particular actions;

(c) meeting with the discloser to discuss the forms of support which may be desired by the discloser and implementing any reasonable forms of support requested;

(d) considering whether the discloser can, or should, be allocated alternative duties or be afforded flexible working arrangements or paid time off work; and

(e) in the discretion of the Company, granting immunity from disciplinary action in respect of any wrongdoing by a discloser which may come to light as a result of making a Protected Disclosure.

10.2 A discloser may contact the Whistleblower Protection Officer, seek independent legal advice or contact regulatory bodies, such as ASIC, APRA or the ATO, if they believe they have suffered detriment.

11 Whistleblower Protection Officer

11.1 The Whistleblower Protection Officer is an employee of the Company who is authorised by the Company to receive disclosures that may qualify for protection under the Corporations Act.

(a) The role of the Whistleblower Protection Officer is to:

(b) handle and facilitate the investigation of Protected Disclosures;

(c) communicate and liaise with a discloser in respect of a Protected Disclosure and any investigation in accordance with this Policy;

(d) provide assistance to a discloser to help ensure their wellbeing;

(e) maintain confidentiality and seek to protect a discloser from any detriment;

(f) answer queries about this Policy and potential disclosures; and

(g) otherwise give effect to this Policy.

11.2 You should inform the Whistleblower Protection Officer if you are being, have been or may be being subjected to detrimental conduct or are concerned that your disclosure has not been dealt with appropriately.

12 Other whistleblower schemes

12.1 There may also be other avenues and legal protections available to persons who have disclosed, or wish to disclose, suspected wrongdoing, which are provided for under other legislation.

12.2 Depending on the nature of the disclosure, such legislation may include, but is not limited to, the tax whistleblower regime under Part IVD of the *Taxation Administration Act 1953* (Cth) or the general protections under the *Fair Work Act 2009* (Cth).

13 Publication of this Policy

To assist in achieving the objectives of this Policy, the Company will take steps to ensure this Policy is readily available to, and understood by, officers and employees, including by:

(a) setting out the Policy in the employee handbook and making the Policy available on the staff intranet and the Company's external website;

(b) incorporating the Policy in board and employee induction information packs and training for new starters; and

(c) conducting training from time-to-time, including specialist training for staff members who have specific responsibilities under the Policy.

14 Definitions

Unless the context otherwise requires, in this Policy:

APRA means the Australian Prudential Regulation Authority;

ASIC means the Australian Securities and Investments Commission;

detriment and **detrimental conduct** includes (without limitation) any of the following:

(a) dismissal of an employee;

(b) injury of an employee in his or her employment;

(c) alteration of an employee’s position or duties to his or her disadvantage;

(d) discrimination between an employee and other employees of the same employer;

(e) harassment or intimidation of a person;

(f) harm or injury to a person, including psychological harm;

(g) damage to a person’s property;

(h) damage to a person’s reputation;

(i) damage to a person’s business or financial position;

(j) any other damage to a person;

Eligible Whistleblower means a person who is, or has been, any of the following:

(a) an officer of the Company;

(b) an employee of the Company (regardless of whether permanent, part-time, casual, fixed-term or temporary);

(c) an individual who supplies services or goods to the Company (whether paid or unpaid);

(d) an employee of a person who supplies services or goods to the Company (paid or unpaid);

(e) an individual who is an associate of the Company; or

(f) a relative of an individual referred to in (a) to (e) above, or a dependant of the individual (or such individual's spouse); or

(g) any other individual prescribed by regulation;

misconduct includes, but is not limited to, fraud, negligence, default, breach of trust and breach of duty;

Protected Disclosure means a disclosure of information which qualifies for protection under Part 9.4AAA of the Corporations Act;

Senior Manager, in respect of a company, means a person (other than a director or secretary of the company) who:

(a) makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of the company; or

(b) has the capacity to affect significantly the company's financial standing; and

Whistleblower Protection Officer means the Human Resources Manager of the Company and such other persons who may be designated as a Whistleblower Protection Officer by the Company from time-to-time.

15 Consequences for a breach of this Policy

Any breach of this Policy by an employee may result in disciplinary action, including termination of employment. A contravention of this Policy may, in some circumstances, also expose a person to criminal or civil liability for a breach of applicable legislation.

16 Review of this Policy

This Policy will be reviewed at least every two years to ensure it remains correct and complies with relevant legislation. The Policy was last reviewed on 29 June 2021.

Schedule 11

Anti-Bribery and Corruption Policy

Way 2 Vat Limited

(Company)

1 Introduction

1.1 Way 2 Vat Limited (**Company**) is committed to conducting all of its business activities fairly, honestly with integrity, and in compliance with all applicable laws, rules and regulations. The Company's board of directors (**Board**), management and employees are dedicated to high ethical standards and recognise and support the Company's commitment to compliance with these standards.

1.2 In particular, the Company is committed to preventing any form of Corruption and Bribery and to upholding all laws relevant to these issues, including the Anti-Corruption Legislation. In order to support this commitment, the Company has adopted this Anti-Bribery and Anti-Corruption Policy (**Policy**) to ensure that it has effective procedures in place to prevent Corruption and Bribery.

2 Scope of Policy

2.1 This Policy applies globally. To the extent that local laws, codes of conduct or other regulations (**Local Laws**) in any countries are more rigorous or restrictive than this Policy, those Local Laws should be followed by any subsidiary operating in that country. Where a country has specific Bribery and Corruption Local Laws which are less rigorous than this Policy, this Policy prevails. The Company may, from time to time, provide country specific directions for subsidiaries operating in countries outside Australia.

2.2 This Policy sets out the Company's requirements in relation to interactions with Officials and Third Parties. This Policy does not prohibit interactions with Officials, rather it forbids corrupt interactions with those individuals.

2.3 This Policy applies without exception and without regard to conflicting regional customs, local practices or competitive conditions to all directors, officers and employees of the Company (**Company Personnel**). Upon commencement of employment or service (as appropriate) and from time to time thereafter (as requested by the Company), all Company Personnel must acknowledge their being bound by, and agreement to comply, with this Policy by executing the attached Certification of Compliance at Annexure A).

3 Definitions

In this Policy the following words or phrases mean the following:

Anti-Bribery Officer means an officer of the Company designated by the Board to receive information from the Board, Personnel or Business Associates of the Company according to the terms of this Policy;

Anti-Corruption Legislation includes many laws such as the *Criminal Code Act 1995* (Cth), the *Penal Law 1977* (Israel), *Economic Competition Law 1988* (Israel) and all other legislation that applies to the Company, regardless of jurisdiction;

Bribery is the act of offering, promising, giving or accepting a benefit with the intention of influencing a person who is otherwise expected to act in good faith or in an impartial manner, to do or omit to do anything in the performance of their role or function, in order to provide the Company with business or a business advantage that is not legitimately due (whether in respect of an interaction with an Official or any commercial transaction in the private sector);

Business Associates means third party companies and individuals (such as joint venture partners, consultants and agents) acting on the Company's behalf, whether directly or indirectly, by representing the Company's interests to foreign governments in relation to international business development or retention of business opportunities;

Company means Way 2 Vat Limited and all of its subsidiaries;

Corruption is the abuse of entrusted power for private gain;

Facilitation Payment means payments of nominal amounts or other inducement made to persons in order to secure or expedite the performance of a Government Official's routine governmental duties or actions;

Gifts, Entertainment and Hospitality includes the receipt or offer of presents, meals or tokens of appreciation and gratitude or invitations to events, functions, or other social gatherings, in connection with matters related to the Company's business unless they:

(a) fall within reasonable bounds of value and occurrence;

(b) do not influence, or are not perceived to influence, objective business judgement; and

(c) are not prohibited or limited by applicable laws or applicable industry codes;

Government Official means:

(a) any politician, political party, party official or candidate of political office;

(b) any official or employee of a domestic or foreign government (whether national, state/provincial or local) or agency, department or instrumentality of any domestic or foreign government or any government-owned or controlled entity (including state-owned enterprises);

(c) any official or employee of any public international organisation;

(d) any person acting in a private or public official function or capacity for such domestic or foreign government, agency, instrumentality, entity or organisation;

(e) any person who holds or performs the duties of any appointment created by custom or convention or who otherwise acts in an official capacity (including, some indigenous or tribal leaders who are authorised and empowered to act on behalf of the relevant group of indigenous peoples and members of royal families); or

(f) any person who holds themselves out to be an authorised intermediary of a government official;

Item of Value includes, amongst other things, cash, travel, meals, Gifts, Entertainment and Hospitality, other tangible or intangible benefits or anything of value;

Money-laundering means the process by which a person or entity conceals the existence of an illegal source of income and then disguises that income to make it appear legitimate;

Official means a Government Official, political party, official or officer of a political party or candidate for political office;

Personnel means all persons acting (whether authorised or unauthorised) on behalf of the Company at all levels, including officers, directors, temporary staff, contractors, consultants and employees of the Company;

Secret Commissions means offering or giving a commission to an agent or representative of another person that is not disclosed by that agent or representative to their principal to induce or influence the conduct of the principal's business;

Secure an improper advantage includes obtaining any commercial or financial benefit; and

Third Party means any individual or organisation other than Officials, with whom Personnel come into contact during the course of their employment or business relationships associated with the Company.

4 Purpose

The purpose of this Policy is to:

(a) set out the responsibilities of the Company and its management and Personnel in upholding the Company's commitment to preventing any form of Bribery or Corruption; and

(b) provide information and guidance to Personnel on how to recognise and deal with any potential Bribery and Corruption issues.

5 Scope and Authority

5.1 The Company requires all Personnel to comply with this Policy as well as the Anti-Corruption Legislation. The prevention, detection and reporting of Bribery and other forms of Corruption are the responsibility of all those working for the Company or under its control.

5.2 This Policy applies to all Personnel, including directors, temporary staff and contractors, and Business Associates of the Company.

6 Responsibility for Policy Compliance and Training

6.1 The Company's Board is responsible for the overall administration of this Policy. The Board and the Anti-Bribery Officer will monitor the implementation of this Policy and will review on an ongoing basis the Policy's suitability and effectiveness. Internal control systems and procedures will be audited regularly to ensure that they are effective in minimising the risk of non-compliance with this Policy.

6.2 A copy of this Policy will be made available to all Personnel via the Company's intranet and in such other ways as will ensure the policy is available to Personnel wishing to use it.

6.3 All Personnel are required to understand and comply with this Policy and to follow the reporting requirements set out in this Policy. To this end, regular and appropriate training on how to comply with this Policy will be provided to all senior managers and other relevant Personnel by the Board and the Anti-Bribery Officer for each business. However, it is the responsibility of all Personnel to ensure that they read, understand and comply with this Policy.

6.4 All Business Associates are required to be made aware of this Policy and to undertake to comply with this Policy in relation to any of their dealings with, for or on behalf of the Company.

6.5 The prevention, detection and reporting of Bribery and other improper conduct addressed by this Policy are the responsibility of all those working for or engaged by the Company. All Personnel should be vigilant and immediately report any breaches or suspicious activity to the officer responsible for compliance.

7 Consequences of Breaching this Policy

7.1 Bribery and the related improper conduct addressed by this Policy are very serious offences that will be taken seriously, reviewed and thoroughly investigated by the Company. Depending on the circumstances, the incident may be referred to regulatory and law enforcement agencies.

7.2 A breach of this Policy may also expose Personnel and the Company to criminal and/or civil penalties, substantial fines, exclusion from tendering for government or private contracts, loss of business and reputational damage.

7.3 Breach of this Policy by Personnel will be regarded as serious misconduct, leading to disciplinary action which may include termination of employment.

8 Policy

Personnel must:

(a) understand and comply with this Policy and attend all relevant training;

(b) not engage in Bribery or any other form of Corruption or improper conduct;

(c) not make Facilitation Payments;

(d) not offer, pay, solicit or accept Secret Commissions;

(e) not engage in Money Laundering;

(f) not give or accept Items of Value where to do so might influence, or be perceived to influence, objective business judgement or otherwise be perceived as improper in the circumstances;

(g) obtain required approvals for political contributions and charitable donations;

(h) maintain accurate records of dealings with Third Parties; and

(i) be vigilant and report any breaches of, or suspicious behaviour related to, this Policy.

(j) This Policy does not prohibit the giving of normal and appropriate hospitality to, or receiving it from, Third Parties.

9 Prohibition Against Bribery and Corruption

9.1 The Company strictly prohibits Personnel engaging in or tolerating Bribery or any other form of Corruption or improper conduct.

9.2 The Company's corporate values require that in all aspects of business all Personnel act honestly, adhere to the highest ethical standards, and act in compliance with all relevant legal requirements. In this respect Personnel must not engage in Bribery or any other form of Corruption.

9.3 The prohibition of Bribery under this Policy includes the provision or conveying of an Item of Value to any Third Party, Official or family members of Officials, whether directly or indirectly, to secure any improper advantage or to obtain or retain business. This means that Personnel must not:

(a) offer, promise or give an Item of Value with the intention of influencing an Official or Third Party who is otherwise expected to act in good faith or in an impartial manner, to do or omit to do anything in the performance of their role or function, in order to provide the Company with business or an improper advantage; or

(b) authorise the payment or provision of Items of Value to any other person, if it is known, or reasonably should have been known, that any portion of that payment or Item of Value will be passed onto an Official or Third Party to secure an improper advantage or obtain or retain business; or

(c) engage, or procure, a third party to make a payment or provide an Item of Value to an Official or Third Party, (or to procure another person to make such payment or provision), in order to secure an improper advantage or obtain or retain business; or

(d) give an Item of Value to an Official to expedite or to secure the performance of a routine governmental action is strictly prohibited. These may include payments to obtain permits, licenses or visas, or to obtain police protection, or facilitate importation of goods.

9.4 The prohibition of Bribery under this Policy also includes the request or acceptance of (or the agreement to accept) an Item of Value from an Official or Third Party either:

(a) intending that, in consequence, a function or activity should be performed improperly (whether by the requestor/acceptor or another person); or

(b) where the request, agreement or acceptance itself constitutes the recipient's improper performance of a function or activity; or

(c) as a reward for the improper performance of a function or activity (whether by the recipient or another person).

10 Gifts, Meals, Entertainment, Travel and Accommodation

10.1 **General rule**

(a) Company Personnel may not, on behalf of the Company, provide or receive any gifts (including cash or cash equivalents), meals, entertainment, travel or accommodation directly or indirectly, to or from a Government Official a Customer Representative or a supplier including a service provider to the Company, or their respective family members if the transaction might improperly induce (or appear to induce) the recipient to use his or her influence to secure an Improper Advantage for the giver. This includes gifts to charities or other organizations in which the recipient or a family member is or might be involved.

(b) Useful tests for determining a gift's inappropriateness are:

(i) if the gift would create embarrassment or obligation for the giver or receiver, or

(ii) if the action could not stand up to public scrutiny.

(c) In receiving gifts, Company Personnel must ask themselves whether one purpose of a gift is intended to influence, or appear to influence, business decisions and would thereby compromise their ability to act in the best interests of the Company.

10.2 **Gifts**

(a) Subject to the above, Company Personnel may give or receive a gift of nominal value to or from a Customer Representative. A gift is considered of nominal value if its retail value is less than $100 or its equivalent. Even if the gift is less than nominal value, Company Personnel should only accept it if it is consistent with common business practice. Any offer to Company Personnel of a gift or other business courtesy that exceeds nominal value, or that seems inconsistent with common business practices, should be immediately reported to the General Counsel.

(b) Company personnel may never give a gift, even of nominal value, to a Government Official.

10.3 **Meals and Entertainment**

Company Personnel may offer or receive infrequent, reasonable and appropriate business meals or entertainment; provided that business is discussed at those events and that the activity has a clear business purpose. An example would be the promotion, demonstration or

explanation of the Company's products or services, or the execution or performance of a contract. Such activity shall not involve excessive expenditures. The guidelines for reasonable and appropriate activities shall be normal industry practice in the relevant locality consistent with local legal requirements. While the gift value described above does not strictly apply in the case of meals and entertainment, that limitation is an indication of the reasonableness of the meals or entertainment.

11 Prohibition On Facilitation Payments, Secret Commissions and Money Laundering

11.1 The Company does not condone the making of Facilitation Payments, Secret Commissions and Money Laundering.

11.2 Personnel are prohibited from:

(a) making Facilitation Payments;

(b) offering, paying, soliciting or receiving Secret Commissions; and

(c) engaging in Money-Laundering.

12 Political Contributions and Charitable Donations

12.1 The Company prohibits Personnel from making political contributions to Officials on behalf of the Company. Any donations above a level determined in Federal legislation must be disclosed annually to the Australian Electoral Commission and will be published on its website.

12.2 This Policy does not seek to curtail an individual's freedom to make political contributions in their personal capacity.

12.3 The context of any other political contributions is key in determining their appropriateness. For instance, it is permissible for the Company to make a payment to attend a political function in circumstances where such payment could not be construed as an attempt to influence the political party.

12.4 If you are in any doubt as to the appropriateness of any political contribution, you should consult the Board or the Anti-Bribery Officer before it is given or accepted or otherwise as soon as possible.

12.5 The Company can only make charitable donations that are legal and ethical under local laws and practices. In order to ensure that donations made by the Company to charitable organisations are for proper charitable purposes, Personnel must only make donations on behalf of the Company to charitable organisations previously approved by the Company and within approved financial limits.

12.6 A list of approved charitable organisations is to be maintained by the Board and provided upon request.

13 Interactions with Officials and Third Parties Must be Compliant

The actions of customers that are channel partners or Agents (**Third Parties**) present particular risks, because in certain circumstances the Company and its employees can be held liable for improper payments made even if the Company did not have actual knowledge of the payment. Furthermore, such improper payments between Third Parties and Government Officials may be used to facilitate money laundering or terrorist financing without the knowledge of the Company. Accordingly, this Policy provides for strict due diligence and controls when dealing with Third Parties who may interact with a Government Official for or on behalf of the Company.

14 Payments and Fees

All payments made to a Third Party must be reasonable in relation to the products sold to, or bona fide services rendered by, the Third Party to or on behalf of the Company. Payments to a Third Party should never be made in cash and should be made to the Third Party's bank account in the country where the services are performed or where the Third Party's offices are located. No payments shall be made to a Third Party without detailed invoices that fully and accurately describe the services and expenses incurred.

15 Due Diligence

15.1 **Due Diligence Overview**

(a) Due diligence must be performed to ensure that a Third Party is a bona fide and legitimate entity, is qualified for the purpose of its engagement, and maintains standards consistent with the ethical and reputational standards of the Company.

(b) Due diligence on Third Parties also minimizes the risk of payments being used to facilitate money laundering or terrorist financing without the Company's knowledge.

(c) The Company recognizes that corruption risks can vary by location, type of transaction and customer, and, accordingly, this Policy requires enhanced diligence procedures for engaging with Third Parties in circumstances that present a higher perceived risk of corruption.

(i) Basic Due Diligence is required for screening all potential Third Parties

(ii) Enhanced Due Diligence is required for all potential Third Parties who may be involved in sales, business development, regulatory approvals or other capacity in the following regions, even if Basic Due Diligence does not identify any 'red flags' or issues of concern: **Russia, CIS, Eastern Europe, the Middle East (excluding Israel), Central and South America, China, Southeast Asia and Africa**.

(iii) Enhanced Due Diligence is required for all potential Third Parties who may **deal with Government Officials** on behalf of the Company;

(iv) Enhanced Due Diligence is required if any **issues of concern** or '**red flags**' are identified in the Basic Due Diligence. Inability or difficulty to verify the corporate history of an entity or the background and expertise of an individual should be considered a 'red flag' that requires Enhanced Due Diligence. Negative reports in the media or in the local business community are also 'red flags' requiring Enhanced Due Diligence. Annexure B contains a list of red flags. You should discuss any 'red flags' concerning a particular potential Agent with the General Counsel.

(d) Annexure C to this Policy provides a flow chart to aid Company Personnel in conducting these due diligence procedures. [1]

16 Basic Due Diligence Steps

16.1 The required Basic Due Diligence includes:

(a) completion of a credit application form (if applicable);

[1] 0 serves only as a guide and does not reflect all facts and circumstances that may arise in the course of due diligence. Company Personnel should contact the General Counsel with any questions or for additional guidance.

(b) verification of the corporate registration of the entity, or the expertise of a person, the business address, corporate history, corporate structure and beneficial ownership, directorships, etc; and

(c) media search to identify any negative publicity (i.e., conducting reasonable key word searches using public Internet search engines).

16.2 Information regarding items (b) and (c) generally can be confirmed through a third party credit report and desktop media searches. Information identified during the background screening will be reviewed by the accounting department and should be maintained in a due diligence file regarding the potential Customer Representative or Business Partner.

17 Enhanced Due Diligence Steps

17.1 The following steps should be taken in connection with Enhanced Due Diligence of a potential Third Party:

(a) **External research and verification of the Third Party's experience and expertise**

Publicly available information regarding the potential Third Party should be verified through independent sources. 0 to this Policy identifies sources that should be considered in conducting background checks of potential Third Parties, and lists factors demonstrating relevant experience and expertise that should be used in evaluating potential Third Parties. A copy of all research and background checks should be maintained in the due diligence file regarding the potential Third Party.

(b) **Completion of a Due Diligence Questionnaire**

In most cases, it will be appropriate to have the prospective Third Party submit responses to the Due Diligence Questionnaire, attached to this Policy as Annexure E. The Due Diligence Questionnaire should be supplemented with additional questions depending on the particular facts and circumstances. A copy of the completed Due Diligence Questionnaire should be maintained in the due diligence file regarding the potential Third Party

17.2 In addition to the foregoing, in person meetings are a useful means of verifying business qualifications, experience and expertise of Third Parties. Where an in person meeting or meetings has occurred, the Company Personnel involved in such meeting(s) should document, in the form of written notes or a brief memorandum, the date(s) of the meeting(s), location(s), participants and the discussion that took place. Such documentation should then be provided to the General Counsel for review and should ultimately be maintained in the due diligence file regarding the potential Third Party.

18 Solicitation, Extortion, Health and Safety

18.1 This Policy prohibits payment even where they have been requested or demanded by a Government Official or if the Government Official threatens adverse action against the Company unless a payment is made.

18.2 If a payment is made to protect an individual's health and safety, it should be immediately reported to the Legal Department and must be accurately recorded in the Company's books and records to reflect the amount and purpose of the payment. If at all practicable, contact should be made with the General Counsel before such a payment is made. If prior consultation is not practicable, the fact of payment and the circumstances should be reported as soon as is practicable thereafter.

19 Documentation and Recordkeeping

19.1 As part of the Company's commitment to open and honest business practice the Company requires all of its businesses to maintain accurate books of account and records.

19.2 The Company and its subsidiaries must keep accurate and complete records of all business transactions:

(a) in accordance with generally accepted accounting principles and practices;

(b) in accordance with the Company's accounting and finance policies; and

(c) in a manner that reasonably reflects the underlying transactions and events.

19.3 It is the responsibility of all Personnel to ensure that all business transactions are recorded honestly and accurately and that any errors or falsification of documents are promptly reported to the appropriate member of the senior management team of the relevant business, and corrected. No accounts are to be kept 'off the books' to facilitate or conceal improper payments.

19.4 All Personnel must record Items of Value given or received in the Items of Value Register as set out in Schedule 1 / in expense reports and approved in accordance with the relevant expense policy.

20 Compliance With Local Laws Required

If Local Laws in a particular country or region are more restrictive than this Policy, then any Personnel, including any Business Associates operating in that country or region must fully comply with the more restrictive requirements.

21 Reporting Violations and Suspected Misconduct

21.1 Any Personnel or stakeholder who believes that a violation of this Policy or any laws has been committed, is being committed, or is being planned, should report the matter immediately to the Board or the Anti-Bribery Officer.

21.2 If anyone is unsure whether a particular act constitutes Bribery, a Facilitation Payment, Secret Commission, Money-Laundering or an improper Item of Value, or has any other queries, they should ask the Board or the Anti-Bribery Officer.

22 Protection

22.1 The Company prohibits retaliation against anyone reporting such suspicions.

22.2 Personnel who wish to raise a concern or report another's wrongdoing, or who have refused pressure to either accept or offer a bribe, should not be worried about possible repercussions. The Company encourages openness and will support any Personnel who raises genuine concerns in good faith under this Policy.

22.3 If you are not comfortable, for any reason, with speaking directly to the Board or the Anti-Bribery Officer, the Company has a Whistleblower Policy which affords certain protections against reprisal, harassment or demotion for making the report.

23 Monitoring and Review

23.1 Records of reports made under this Policy will be maintained and reviewed by the Audit Committee periodically.

23.2 The Board and the Anti-Bribery Officer will monitor the content, effectiveness and implementation of this Policy on a regular basis. There may also be independent reviews taken from time to time. Any findings, updates or improvements identified will be addressed as soon as possible.

23.3 Personnel are invited to comment on this Policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the Board or the Anti-Bribery Officer.

24 Reporting and Disciplinary Action

24.1 Failure to Comply and Disciplinary Action

All persons subject to this Policy shall comply with the Policy and promptly report any known or suspected violations of this Policy, as well as any other illegal, improper or unethical conduct, pursuant to the procedures described below. The Company will view any violation of this Policy or failure to report a violation as a significant matter that warrants disciplinary action and may impose such sanctions as it deems appropriate, including, among other things, a letter of censure or suspension or termination of the employment or services of the violator.

24.2 Reporting Violations and Anonymous Complaints

(a) Any transaction, no matter how seemingly insignificant, that might give rise to a violation of the Policy and/or applicable anti-corruption laws and regulations must be reported promptly to a supervisor or manager, or the General Counsel.

(b) If you wish to remain anonymous, you may report a violation of this Policy by contacting the Company's General Counsel.

(c) All such reports may be made in person or by letter, telephone, facsimile, e-mail, or other means and will be treated as confidential, to be used only for the purpose of addressing the specific problem(s) the reports concern. Such reports will be shared with the Company's management and other authorized individuals only on a need-to-know basis. All persons subject to this Policy shall cooperate fully, truthfully, and candidly with any inquiry conducted by or on behalf of the Company. Failure to provide such cooperation may result in discipline, including termination of employment.

Annexure A

Way2Vat Ltd – Anti-Corruption and Bribery Policy

Certification of Compliance

I, _____, have received a copy of, read, and am familiar with the Company's Anti-Corruption Policy (the **Policy**). I hereby agree to comply with the specific requirements of the Policy in all respects during my employment, my service on the Board of Directors, or other service relationship for or with the Company, and thereafter to the extent required by the Policy. I understand that any activity in violation of the Foreign Corrupt Practices Act or other applicable anti-corruption laws and regulations is prohibited, and I understand the possible consequences of a violation. I am presently in full compliance with the Policy, and I know of no clear violations of the Policy by any other entity or person subject to the Policy, except as previously reported to the Company. I recognize that failure to comply in all respects with the Policy may be a basis for termination for cause of my employment or termination of my service relationship with Way 2 Vat Ltd.

_____

Signature

_____

Date

Annexure B

Red Flags

All Company Personnel should be aware of 'red flags' that may indicate questionable transactions that expose the Company to legal, financial, or reputational harm. 'Red flags' include, without limitation:

1 Unusual payments or financial arrangements such as:

(a) Payments to a bank account without the disclosure of the person's or organization's name associated with the account, and/or to a bank account in a different name than the person or organization entitled to payment from the Company;

(b) Payments to accounts in countries other than where the agent is located or business is to be performed; or

(c) Cash or non-cash in-kind payments.

2 Unusually high commissions in net value or in comparison to the value of the contract achieved.

3 Unusual or excessive gift, entertainment, meal or travel expenses.

4 History of corruption in the country.

5 The person or organization has a reputation for paying bribes, or requiring that bribes are paid to, or has a reputation for having a 'special relationship' with, Government Officials.

6 The person or organization insists on the use of side letters or refuses to put the agreed terms in a written document.

7 The person or organization insists on receiving a commission or fee before committing to sign a contract with the Company or carrying out a government function or process for the Company.

8 Use of a person or organization for the purpose of avoiding knowledge of how interactions with Government Officials occur or how problems are resolved.

9 Refusal by a person or organization to certify or agree to contract language that they will not take action that would violate the applicable anti-corruption laws and regulations.

10 'Recommendations' of a person or organization that come from a Government Official.

11 Complex group structures without obvious explanation.

Annexure C

Due Diligence Flow Chart

Basic Due Diligence
(Required for all potential Customer Representatives and Business Partners)

1. Complete the Company's Credit Application Form (if applicable)
2. Verify the corporate registration of the entity, or the expertise of a person, the business address, corporate history, corporate structure and beneficial ownership, directorships, etc., using a third party credit report or equivalent.
3. Conduct a media search to identify any negative publicity (i.e., conduct reasonable keyword searches using public Internet search engines).
4. Submit information gathered from steps 1-3 to the Company's accounting department or General Counsel

Will the potential Customer Representative or Business Partner be involved in sales, business development, regulatory approvals or other capacity in **Russia, CIS, Eastern Europe, the Middle East (excluding Israel), Central and South America, China, Southeast Asia or Africa**?

Yes

Notify the accounting department and/or General Counsel that Enhanced Due Diligence is required.

Enhanced Due Diligence

Work with the accounting department and/or General Counsel to:

1. Conduct external research and verification of experience and expertise. *See* 0.
2. Complete a Due Diligence Questionnaire. See □.
3. Take other action as necessary, which may include documenting in-person meetings.

No

Were any 'red flags' or issues of concern identified?
For example:

- The potential Customer Representative or Business Partner will deal with government officials on behalf of the Company
- Inability or difficulty verifying corporate history or background and expertise
- Negative media reports
- Unusual or excessive payment requests (i.e., requests for over invoicing, up-front payments, unusual commissions or midstream compensation payments)
- Requests for payments in a different country, to a third party, to a bank account outside of the country of operation, or in cash or other untraceable funds
- Refusal or hesitancy to promise in writing to abide by the Company's Policies and governing law
- Charges for violation of local or foreign laws or regulations concerning the award of government or other contracts
- A close relationship with a Government Official or commercial counterparty
- A demand or strong suggestion by a Government Official or commercial counterparty to retain the entity/ individual
- A desire to keep representation of the Company or the terms of the retention secret

Yes

Discuss red flags and issues of concern with the accounting department and/or General Counsel and notify them that Enhanced Due Diligence

No

Notify the accounting department and/or General Counsel that there were no red flags or issues of concern identified.

Annexure D

Background Investigation Checklist

Resources for external verification of a Customer Representative or Business Partner's reputation, experience and qualifications could include:

- A report on candidate's character and reputation by those employees who have met him or her
- A report on candidate's character and reputation based on outside sources:
    - Third party business intelligence providers
    - U.S. State Department country desk or similar source
    - U.S. Commerce Department country or business desk or similar source
    - Commercial Attaché at U.S. Embassy in local country or similar source
    - Commercial office of the foreign embassy in the United States or similar source
    - Chamber of Commerce office
- Bank References
- Screening against databases of politically exposed person and 'watch lists' for sanctioned persons, for example:
    - U.S. Department of State List of Statutorily Debarred Parties: http://www.pmddtc.state.gov/compliance/debar.html or similar source
    - U.S. Office of Foreign Assets Control Specially Designated Nationals List: http://www.treas.gov/offices/enforcement/ofac/sdn or similar source
- A report on family or business ties to government officials
- A report on prior government service
- Verification that candidate has experience in the area for which he or she is being hired
- Assessment of reasonableness and comparability of proposed compensation or profit arrangement
- Opinion of local counsel on possible issues of local law

Evidence of Customer Representative or Business Partner Experience and Expertise

Factors that indicate relevant experience and expertise that should be used in evaluating potential Customer Representatives or Business Partners include:

- A good reputation for ethical behavior, business competence, and reliability
- Financial stability (i.e., adequate resources necessary to accomplish the objectives of the agreement)
- Knowledge of applicable legal procedures and laws
- Adequate facilities for providing service and, as necessary, goods
- The ability to keep pace with expanding business opportunities
- Good access to information within the industry and financial sectors

- An established presence in the local business community

Annexure E

Due Diligence Questionnaire

to be completed by potential Customer Representative or Business Partner

1 Company Name _____

2 Previous Names (if any) _____

3 Country where work will be performed _____

4 Address _____

Telephone _____ Fax _____

5 Entity type and jurisdiction (eg, limited liability company, partnership etc)

_____

6 Date & place of incorporation _____

7 Management information

Chairman/president _____

Managing Director _____

Sales Director _____

8 Ultimate beneficial owners/principals:

Name _____ %Ownership _____

Name _____ %Ownership _____

Name _____ %Ownership _____

Name _____ %Ownership _____

9 Members of the Board of Directors

Name _____

Name _____

Name _____

Name _____

10 Parent Company(ies) _____

Subsidiary Companies _____

Jointly Owned Companies _____

11 Business References

(a) _____

(b) _____

(c) _____

12 Banking/Credit References

(a) _____

(b) _____

(c) _____

13 Percentage of your time which will be devoted to the Company business: _____ %

14 Historical Background:

(a) Years company has been in business

(b) How long have you been involved in the business of

(c) Briefly describe the establishment of your business, the primary areas of business activity, changes in ownership, changes in areas of concentration, growth plans, potential new markets, etc

15 Briefly describe the experience and qualifications of the management personnel of your business and how this relates to this position

16 Please attach financial statements (audited, if available) for the past three (3) years, including balance sheets and profit and loss statements

17 Please use this space to provide any additional information which you feel may be relevant to your qualifications for the position:

18 (a) (i) Does any current or former government official, political party official, candidate for political office, or relative of such a person, have an ownership interest, direct or indirect, in your company?

Yes ☐ No ☐

(ii) Is any former or current government official, political party official, candidate for political office, or relative of such a person, an employee, officer or director of your company?

Yes ☐ No ☐

(b) If the answer to either (a)(i) or (a)(ii) above is yes, please state:

(i) The name and official position of the government or political party official or candidate:

(ii) The official duties and responsibilities of the government or political party official or duties related to the office for which such person is a candidate:

(iii) (a) Indicate the type and extent of the ownership interest in your company of the government or political party official or candidate:

(b) Indicate the position of the government or political party official or candidate, or the relative of such person, with your company:

(c) If the government or political party official or candidate in question is a relative of an owner, employee, officer or director of your company, state the relationship of that official to your owner, employee, officer or director:

_____

_____

_____ _____

Signature Date

_____

Typed name and title

_____

Company

Schedule 1

Items of Value Register

1 Definitions

Gifts, Entertainment and Hospitality includes the receipt or offer of presents, meals or tokens of appreciation and gratitude or invitations to events, functions, or other social gatherings, in connection with matters related to the Company's business unless they:

(a) fall within reasonable bounds of value and occurrence;

(b) do not influence, or are not perceived to influence, objective business judgement; and

(c) are not prohibited or limited by applicable laws or applicable industry codes; and

Item of Value includes, amongst other things, cash, travel, meals, Gifts, Entertainment and Hospitality and other tangible or intangible benefits or anything of value.

2 Completing the Items of Value Register

The following information is required in completing the Items of Value Register:

Receiving Items of Value
Date Received
Name, Position & Business Unit of Recipient
Name of Giver (Who is giving you the gift / entertainment)
Description of gift / entertainment
Value $
Reason for acceptance
Decision on what will happen to gift / entertainment
Name and Position of Approving Manager (eg, GM)

Offering Items of Value
Date Offered
Name, Position & Business Unit of Offeror
Name of Receiver (Who are you offering the gift / entertainment too)
Description of gift / entertainment
Value $
Reason for offering
Decision on what will happen to gift / entertainment
Name and Position of Approving Manager (eg, GM)

Schedule 12

Information Security Policy

Way 2 Vat Limited

(Company)

1 General

1.1 Most foreign Value Added Tax (**VAT**) is left unclaimed by businesses. This is due to highly bureaucratic and complicated reclaim processes, and simply because businesses are not aware that VAT reclaim is possible.

1.2 As a Fintech company, the Company's B2B2E application is revolutionizing the way VAT is reclaimed by companies conducting business in foreign countries and regions. The Company aims to transform a complicated, tedious, and highly bureaucratic process into a seamless one that increases a company's bottom line – with market potential estimated at US$20 billion of unclaimed foreign business VAT each year.

2 Definitions

Audit Trail means an audit log of actions performed on IT and infrastructure systems as a file or as a part of the system. The audit log connects between the actions to other data, such as username of the action performer, time, etc;

Identification means to identify a person \ system while attempting access and authorizing processes in an IT system;

Information Asset means file or information system containing company information;

Information means data stored in writing \ print \ magnetic device \ optical device or any other means;

Information Security Management System (**ISMS**) means a long term framework that aims to enhance information security throughout the organization. (Part of ISO27001 framework);

Information Security Manager means an employee of the information security appointee that acts as a professional guide for all aspects of information security (physical and logical);

Information Security means all technological and organizational means used to mitigate risk pertaining to the confidentiality, integrity, and availability of information stored in IT systems;

Information Security Work Plan means annual work plan, approved by the company's management, which includes information security activities to be performed throughout the year. The plan includes budget estimation for each activity;

ISO27001:2013 means a leading information security standard, detailing how an organization should manage its Information Security Management System (ISMS);

Password means a string of characters known only to the user, used for identification confirmation of the user. Typed as part of the user identification process while logging on;

Policy refers to this Information Security Policy.

Restricted information means data defined by local information privacy legislation in each of the subsidiaries countries or as defined by Company, in subordination to the Israeli Information Privacy Act of 1981;

Sensitive Information means data defined as sensitive by the company's management (Intellectual property);

Storage Media means media used for information storage. Computerized information stored on magnetic or optical media;

User means Company or outsourcing employee that uses the company's information systems for his work. Each employee has a personal username;

Username means a unique identification string provided to each network \ system user in order to verify identity; and

VAT means Value Added Tax.

3 Purpose, Overview and Applicability

3.1 Purpose

The responsibility for Information Security on a day-to-day basis is every employee's duty. In complying with this Policy, the Company decreased the ever-growing threat to our information systems. As new threats arise and vulnerabilities change, so will this Policy. This Policy does not conflict with any official duties of end users, but protect them and our assets from unauthorized and damaging use. The purposes of this Policy is as follows:

(a) ensure that the Company's information resources are appropriately protected from destruction, alteration, or unauthorized access;

(b) ensure that this protection is accomplished in a manner consistent with the business and work flow requirements of the Company;

(c) ensure that the industry's best security practices are implemented in order to reduce vulnerabilities, increase safety, and provide guidance to the company on the expected threats; and

(d) provide a concise set of standards in order to attain consistency across the entire information infrastructure in regard to securing systems and networks.

3.2 Overview and applicability

(a) This Policy:

(i) covers the best security practices to protect all of the Company's information system resources and information;

(ii) applies to:

(A) all Company's personnel including, but not limited to, employees, contractors, consultants, and temporary personnel; and

(B) all outsourcing firms that perform services for the Company.

(b) All the Company's personnel are expected to become familiar, and comply, with this Policy. Personnel, who are not in compliance, are subject to disciplinary actions, including termination.

4 Board and Management Commitment

4.1 The Company's management and board of directors are committed to maintain a high level of information security by their responsibility for proper management of the Company.

4.2 The management is obligated to provide adequate resources to maintain an appropriate level of information security in the Company and to budget the annual work plan.

5 Policy Goals

5.1 This Policy has the following aims:

(a) protecting the Company's information and customer's information from unauthorized and malicious activity by effectively and efficiently enforcing an information security policy;

(b) supporting the business strategy through security guidance and risk management in the manner it is implemented and maintain services for the customers;

(c) maintaining the confidentiality, integrity, and availability of information;

(d) providing the basis for information security procedures and controls;

(e) meeting information security requirements through taking action that ensures the implementation of an appropriate level of information security;

(f) locating and managing risks and exposures of information stored in the system, including prints, scans, tapes, or other hardcopies;

(g) defining tools that actively enhance security awareness to the company management, employees, and suppliers;

5.2 The Company must prepare an annual work plan that includes the following actions:

(a) purchasing, installing, and integrating security products;

(b) maintaining information security products;

(c) maintaining a risk assessment program; and

(d) performing special projects.

6 Information Security Business Principles

This Policy is underpinned by the following key principles:

(a) creating a security culture through information security governance.

(b) assessing risks through understanding, evaluating, and testing.

(c) ensuring effective implementation of the critical information security basics by following policies, procedures, and guidelines.

(d) enforcing the information security policy through education, monitoring, and metrics.

(e) adhering to applicable regulatory requirements that include international and state laws and regulations.

7 Major Risks

7.1 The Company has information of a business, financial, and personnel nature. Unauthorized access or a security breach may affect the confidentiality, integrity, and availability of that information. The major risks associated with a breach of this information is detailed below with relevant examples.

7.2 **Technological risks**

(a) Decrease in availability and credibility of the systems as a result of full or partial damage.

(b) Low performance rate of computers either from internal or external security breaches.

(c) Harm to privacy of company's employees or customers and outside factors, whose details are stored in Company systems, as a result of information disclosed to unauthorized individuals.

(d) Data corruption in production environment information systems, which could cause lead to invalid actions or faulty decision taking.

(e) Harm to the survivability of the company's systems due to technical failure or damage.

7.3 **Human and organizational risks**

(a) A security breach pertaining to employees, customers, internal research and development documentation and specifications, financial data, intellectual property, etc.

(b) Unauthorized access to company's sites and secure\restricted areas.

(c) User error leading to information security breach.

(d) Infiltration of criminal or hostile factors to the company.

(e) The transfer of certain types of information in an insecure manner and\or to unauthorized factors.

(f) Physical damage to hardware and communication equipment.

(g) Loss or theft of stationary or portable IT equipment and sensitive Information.

(h) Failing to comply with applicable legal or regulatory requirements.

8 Key elements in establishing an ISMS

8.1 In general, information security measures and methods are implemented to minimize risks and shall be adapted based on the risk and sensitivity level over time.

8.2 The four key elements implemented to achieve effective information security protection are:

(a) **Prevention** – information security components are designed to prevent malicious or accidental damage to company's information by employees or outsourcers, such as access control systems, authorization systems, and Anti-Virus software;

(b) **Detection** – detecting breaches that were not identified by the prevention layer;

(c) **Reaction** – a reaction (or correction) layer that may be independent or as part of the detection layer which allows response to the breach as a function of the event as a result of a:

(i) real time reaction – by changing the prevention capabilities of the system; and

(ii) post event reaction –based on information logged during the event, analyzing it, and drawing conclusion; and

(d) **Documentation** – the documentation layer shall allow analyzing the events (prevention, detection, or reaction events) to allow a broad perspective of the event.

9 Organizing Information Security

9.1 In order to perform the requirements of the policy, the company shall define a suitable infrastructural framework, based on the following:

9.2 **Information security steering committee**

(a) The information security steering committee (**Steering Committee**) is the highest body authorized to approve initial changes to the policy and to decide how to implement it as a representative of the management and technological factors, while assisting in external consultants and specialists.

(b) The Steering Committee will be composed of the:

(i) IS Manager;

(ii) CEO;

(iii) COO;

(iv) IS Manager; and

(v) HR manager.

9.3 **The committee roles**

(a) Approving the information security policies and procedures and overview implementation.

(b) Approving and monitoring the annual work.

(c) Approving information classification levels and setting the required security level for the Systems.

(d) Be a deciding authority in cases of disagreement in information security subjects.

(e) Update in information security breach events and discussing appropriate reaction.

(f) The Steering Committee shall convene quarterly for an information security overview.

9.4 **IS Manager Responsibility**

(a) Definition and development of security processes and tools in the field of information systems.

(b) Definition, development and integration of processes and tools related to information security.

(c) Information Security audits conduct.

(d) Definition of Information Security levels of the IS and its components in compliance with decisions of the management forum.

(e) Examination of Information Security aspects during jobs definition and suitable authorizations structure.

(f) Development of processes and tools for enforcing and controlling the IS System.

(g) Involvement in technological changes in computer systems, to whatever degree necessary.

(h) Control, supervision and enforcement of the application of all Guidelines and Procedures and company compliance with the legal requirements, regulations and special rules related to information security.

(i) Training and enhancing awareness of Information Security among of the managers and employees in the Company.

(j) Handling of response to security incidents and malfunctions.

(k) Specification of processes and methods concerning levels of sensitivity and information classification to which third parties may be exposed.

(l) Maintaining and updating the Information Security procedures file.

9.5 **IS manager Competence**

(a) Lead process IS incidents and events while performing investigate and learn lessons.

(b) Disconnect users / injury in the process of servicing if there is risk of damage to the databases / information system of the Company.

(c) Initiation of disciplinary proceedings in front of the CEO as required.

10 Data classification

The company has two classes of data: Company Confidential Information and Public information.

10.1 **The Company Confidential Information**

(a) Information in this class is confidential within the company and protected from external access. If such information were to be accessed by unauthorized persons, it could influence the company's operational effectiveness, cause a financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence and reputation. External access to this information is to be prevented, but should this information become public, the consequences are not critical.

(b) Customer Confidential Information - customer's information that is provided to the company by customers under executed non-disclosure agreements. All such customer confidential information should be protected from external access. If such information were to be accessed by unauthorized persons, it could influence the company's operational effectiveness, cause a financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence and reputation.

10.2 **Public**

(a) Information on these systems could be made public with the approval.

(b) This does not include any information that could be used for competitive purposes against the company.

10.3 Customer Confidential Information shall be registered as required by The Israeli Law, Information and Technology Authority or as otherwise required by applicable law.

10.4 As part of general purpose of ensuring the security of documents, all documents in the fields of the company are set as confidential documents.

11 Risk Assessment approach

11.1 A periodic risk assessment is the basis for an ongoing information security activity. The assessment is applied to both the technological and non-technological aspects of information security. The assessment shall be based on documented criteria that divide the information systems to three risk levels: high, medium, and low risks.

11.2 Risk assessment and risk surveys shall include internal and external tests, penetration tests, questioners etc, and shall represent risks based on the potential risk and occurrence likelihood. The assessments and surveys shall be performed in accordance to business requirement and professional advice.

11.3 The risk assessment shall aid with building the work plan that aims to minimize organizational and technological risks, as well as plan specific IT activities.

12 Security of Human Resources

Aspects of information security are implemented by the Company in all the procedures and stages of employment of workers, as specified hereunder:

12.1 **Prior to the Employment of Workers**

(a) It is within the responsibility of the Company to assure that workers of the Company and third-party workers (contractor's workers) are suitable for the position intended to them and understand the responsibilities imposed on them, in order to prevent events of failure, fraud or abuse of information and assets of either the Company and/or its customers.

(b) The management of the Company shall define with respect to each of its office holders:

(i) the necessary qualifications;

(ii) responsibility and authority;

(iii) requirements of reliability;

(iv) access rights to information systems.

(c) The reliability of workers of the Company shall be examined prior to their absorption, through questioning of recommenders. An examination by means of external parties shall be carried out as necessary and according to the decision of the CEO of the Company.

(d) Each employee, at any hierarchic level whatsoever, shall sign a confidentiality agreement, whereby he will maintain the rules of information security, as a condition to his work with the Company.

(e) Prior to commencement of work with the Company, the new employee will undergo guidance, in order to become familiarized with the Company, its policy and with the documents of quality and information security.

12.2 **Within the Process of Employment of Workers**

(a) It is within the responsibility of the management of the Company to assure that workers of the Company and third-party workers are aware of threats of information security, the responsibility and authority imposed upon them, and also that the information security policy and the procedures derived wherefrom are known to them, pursuant to the prevention of any failure in the security of information either erroneously or maliciously.

(b) The Information Security Manager is responsible for the holding of periodic trainings to all the workers of the Company, at all levels of the Company, in order to increase their awareness of the following issues:

(i) quality policy and information security policy;

(ii) familiarization with possible risks and threats to the Company and to the information;

(iii) proper and ethical utilization of assets of the Company;

(iv) manner of protection against possible failures;

(v) manner of conduct upon occurrence of an exceptional event;

(vi) proper and correct use of protections and controls;

(vii) rules of usage of information systems of the Company.

(c) The Information Security Manager is responsible to ascertain that all the workers receive training in information security at least once a year, while examining the effectiveness of trainings and qualifications, which were executed.

12.3 **Completion of Employment or Change of Positions**

(a) The management of the Company is responsible to assure that workers, contractual workers or third-party users of the information systems will leave the organization or change positions in an ordered and safe manner.

(b) Upon transition from one position to another, the managerial team of the Company is responsible to verify that the reliability and trustworthiness of the worker indeed suits the new position.

(c) Upon transition between positions, access authorizations and controls, which were given to the worker in his previous position, should be examined in light of the new authorizations allotted to him. As a default, the authorizations of the previous position shall be blocked, and new authorizations will be opened to the employee, befitting the new position.

(d) As the worker leaves the Company due to whatever cause, the managerial team should verify that:

(i) all his possibilities to access information, supporting systems and assets from the Company or outside of it were blocked;

(ii) the worker returned all the assets and equipment that belong to the Company (computer equipment, documents, etc);

(iii) the worker received guidance with respect to his commitment to the information of the Company and its immunity.

13 Communications Security

13.1 **Information protection**

(a) The internal IP addresses, configurations, and related system design information for the company information systems must be restricted so that both systems and users outside of the company's internal network cannot access this information.

(b) If users leave their computers powered on during non-business hours, they must log out of the network. If users leave their information systems unattended, they must have password protected screen savers or their screen must be locked.

(c) All workstations and laptops must have some form of software-based firewall with intrusion prevention and an Anti-Virus software running at all times on the system.

(d) Any attempt to disable these controls shall be monitored by IT department. If the user disables these controls for any unapproved reasons, and such actions cause damage to the company's resources, such as a virus outbreak, the user can face disciplinary actions up to and including termination.

13.2 **Firewalls and encryption**

(a) All the company's information systems must be located behind a firewall. The only exception to this is external Internet routers or systems approved by the Information Security Officer. All unauthorized and unused ports shall be closed on the firewall. All

open ports have a specific source and destination addresses, except for publicly accessed addresses.

(b) All systems that store the Company's Confidential Information or Customer Confidential Information must be on an internal extranet with firewall protection and have no way of routing to the public Internet or sources.

(c) All Internet web services must employ unique digital certificates and use encryption to transfer information in and out of these devices.

(d) If a methodology for secure channel connection is available (ie, technically feasible), privileged access must be performed over secure channels.

(e) Firewall rules review and administrator's access should be approved once a quarter by the information security officer (same as all networking equipment).

13.3 **Vulnerability assessment and security patches**

(a) All servers must go through proper hardening procedures by authorized IT personnel before they are connected to the company's network. Once the servers are hardened, they must go through a vulnerability assessment by the IT department. After risk analysis has been performed on all identified vulnerabilities, all exceptions must be documented and reviewed on a quarterly basis by the information security officer. The only exception to this policy are servers that are in a controlled development lab environment. A controlled development lab environment must be located on a separate VLAN from the production network with access control lists and monitoring in order to control data traffic to the production network.

(b) All servers must have current security patches loaded within a reasonable amount of time after the patch release in order to be protected from current vulnerabilities and threats. The IT department is responsible for notifying system administrators of new patches and upgrades, as well as all other vulnerability fixes that are required.

(c) An external security audit shall be performed on an annual basis to ensure that the company is following industry standards for network security. This also assists the company with identifying any security threats that the company might not be aware of. The IT department is responsible for delivering these reports to the proper managers for corrective actions.

(d) On a weekly basis, the IT department must review all security advisories and bulletins issued by trusted sources.

13.4 **Intrusion detection**

(a) Perimeter-based intrusion detection is required at all Internet access points on the network. These sensors must be monitored 24/7 in order to detect attacks, penetration attempts, network probing, network scanning, and unauthorized actions against the company's networks.

(b) Host-based intrusion detection is required on all servers, network nodes, and all other critical systems.

(c) For information systems, the IT department must prepare, periodically update, and regularly test the intrusion response plan. This plan must provide for the continual operation of critical systems in the event of an interruption, degradation, or compromise of services.

(d) Whenever an employee has a good reason to believe that an information system has been compromised, the employee should report the incident to the IT department in accordance with the reporting of security incidents procedures. The only exception to this policy is if the system causes immediate damage to the company's resources, and in which case, the system is to be disconnected from the network.

13.5 **Training and awareness**

(a) Every Worker will attend an annual information Security awareness class. To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions.

(b) Every new worker must attend an information security awareness class within one (1) month of his commencement of employment at the company. To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions.

(c) The IT department must provide refresher courses and other such materials to regularly remind all workers about their obligations with respect to information security.

14 Network Access

14.1 **Requirements for network access**

(a) All users must go through proper security training and sign an end-user agreement prior to gaining access to the network.

(b) Authorized IT personnel must attach all new workstations and servers to the network, including uncontrolled development lab environments. Likewise, all new user accounts and new needs for access rights must be created and maintained by authorized IT personnel. IT department must ensure that all systems have current patching and Anti-Virus controls installed.

(c) All software that is run on any company system must be approved and installed by the IT department. Any attempt to install unauthorized software is strictly prohibited and can lead to disciplinary actions.

(d) All new extranet connectivity shall undergo a security review by the information security officer. The reviews are to ensure that all access matches the business requirements in the best possible way. All proposed connectivity must be submitted through the change management process.

14.2 **Requirements for VPN access**

(a) All users, who remotely connect via VPN, must be authorized. For access, strong user authentication must be used, which includes a user-id and a password.

(b) All remote VPN users shall have their VPN and software-based firewall installed and running (Microsoft or the Anti-virus client firewall).

14.3 **Requirements for wireless access**

The use of wireless access to visitors of any kind is authorized only if the wireless entry point is on the external side of the firewall and network-based intrusion detection is used.

14.4 **Requirements for video access**

All the company's video equipment shall be deployed on the trusted side of their respective firewall. They shall not have connections bypassing the firewalls. They shall be configured with a non-default password. They shall have the most current versions of the software and patches per vendor website.

15 System Access Control

15.1 End-user passwords

(a) Passwords to all the company's information systems must be at least six (8) alphanumeric characters. Passwords must include at least one lower case letter and one number.

(b) Special characters. All user-chosen passwords must be difficult to guess. Dictionary words, derivatives of user-ids, and common character sequences, such as abc123, shall be denied.

(c) End-user passwords must be changed once every three months or terminated when an end-user no longer requires access to systems, whichever happens first. When changing passwords, they must be different from the previous passwords and adhere to the format described above.

(d) Passwords must not be written down or stored in an insecure place. Passwords must not be stored in a readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.

(e) Passwords must never be shared with unauthorized users. To do so exposes the authorized user to responsibility for the actions that the other party performs with the disclosed password.

(f) All passwords must be changed immediately if they are suspected of being disclosed, or have known to have been disclosed to anyone besides the authorized user.

15.2 Critical systems and domain administrator passwords

All critical systems and domain administrator accounts must be limited to authorize administrators only. The IT department shall test all privileged account passwords for strict compliance with this policy. Each administrator must have his rights reviewed once every quarter by his respective manager and approvals must be forwarded to the IT department. Any misuse or unauthorized use of a privileged account or unauthorized information systems access shall result in punishment up to and including termination.

15.3 Password system set-up

(a) All information systems permanently or intermittently connected to the company's networks must have password access controls. Multi-user systems must employ user-ids and passwords unique to each user, as well as user privilege restrictions. Systems must also have password protected screen savers or screen locks when the system is unattended. Upon assignment of new user accounts, a default password shall be used. The user must be forced to change the password after the first login.

(b) When creating and maintaining user accounts, the principle of least privileges required to perform a function must be used when granting permissions.

(c) All default passwords shall be changed immediately after product installation.

(d) Only trained members of the IT Department will be allowed to have administrative rights to the network servers and systems. The information Security Officer and the Director of IT must approve all administrative rights. The only exception to this is official third party users, who have first been authorized by the VP product manager.

15.4 Log-in/ log-off process

(a) Access to the company's network is restricted to authorized users only. An authorized user is any user, who has a valid network account and has been given login rights to the network.

(b) All new users must have their manager sign a 'Network Access Request ticket' and forward it to the Help Desk, who grants access. The exception to this policy is administrative and privileged accounts.

(c) Access for non-company's employees, such as contactors or third parties, must be re-authorized for a period longer than 90 days. If an extension is needed, the manager responsible for the access must request the extension in writing to the Information Security Group.

(d) The user's immediate manager must re-evaluate the system privileges granted to every user every 180 days. This re-evaluation involves a determination whether currently enabled system privileges are still needed to perform the user's current duties.

(e) Users must not use their information systems for unofficial use. This includes participating in chat-rooms, bulletin boards, personal newsgroups, sharing files like using peer2peer mp3 sharing sites, downloading unauthorized software for unofficial use, and inappropriate use of the Internet.

(f) Access from remote sites must either be through dial-up using the iPass client or an approved encrypted method, such as SSL or VPN. At no time should an un-encrypted packet with user login information leave or enter the network.

(g) There shall be no open shares on any workstation or laptop file systems. All shared directories must be authenticated and be used for official purposes only. Whenever possible, company file servers should be used to store and grant access to data, not individual workstations. Sensitive information that is created or used on workstations and laptops should be stored on company fileservers whenever available. All sensitive information that is stored on workstations and laptops when company file servers are not available should be encrypted and stored in password-protected directories.

15.5 **Information systems access privileges terminate when users leave**

(a) When authorized users are terminated or leave the company, their access must immediately be terminated. This includes all network login accounts, remote access accounts, and system administration level accounts. All root and administrative passwords known to the individual must also be changed.

(b) The Human Resources department shall notify IT department of new/terminating employees by submitting a 'New/Terminating Employee Notification Form'. Under all circumstances, IT department is to be notified by completing the form and submitting to the IT department.

15.6 **Gaining unauthorized access via the company's information systems**

(a) Authorized users must not use the company's information systems in order to give access to other information systems to which they do not have authorized access. This includes damaging, alerting, or disrupting any operations of the company's information systems. Likewise, users are prohibited from capturing or obtaining passwords, encryption keys, or any other access control method, which would permit them with unauthorized access.

(b) Users must not scan for or exploit vulnerabilities or deficiencies in information systems security in order to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted. All such vulnerabilities and deficiencies should be promptly reported to the IT department in accordance with the reporting of security incidents procedures.

16 Application Security

16.1 Application access control

All applications that process, store, or transmit information other than public information must have user authentication other than normal domain access. These applications must be accessible only to authorized users.

16.2 Application firewalls

All applications that are accessible to an external network and are intended for public use, such as online services, must have a web-application-based firewall in addition to a network-based firewall in order to prevent unauthorized users from exploiting vulnerabilities and/or gain unauthorized access through the applications.

16.3 Internal\external applications vulnerability testing

All applications that are accessible to an external network and are intended for public use, such as online services, must go through an application vulnerability assessment in order to identify known exploits. All applications that process, transmit, or store privacy information must have all vulnerabilities identified and corrected.

17 Electronic Mail Systems and Internet Usage

17.1 Electronic mail systems

(a) Users must not use an e-mail account assigned to another user to either send or receive messages. Authorization from the e-mail assignor may give delegated users access to their inbox for official purposes.

(b) When users receive unwanted or unsolicited e-mails (also known as spam mail), which contain a virus or malicious code, they must refrain from directly responding to the sender. Instead, they should call the help desk, which shall work with the IT department that shall take the appropriate actions.

(c) Users must not create or forward e-mails with the Company's Confidential Information or Customer Confidential Information unless encryption is used. Likewise, if a contract is e-mailed, it must be write-protected so the end user cannot make unauthorized changes.

17.2 Internet connections

(a) Although the Internet is an informal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. To this end, users of the company's information systems must for example (1) repost material only after obtaining permission from the source, (2) quote material from other sources only if these sources are identified, and (3) reveal internal company's information on the Internet only if the information has been officially approved for public release. This also forbids the online trading of copyrighted material. An example of this is file-swapping copyrighted material through the Internet.

(b) Users must not place any company's materials on any publicly accessible Internet computer system unless the CEO first approved the posting.

(c) Users must not accept any attempts from websites that wish to install software or change settings on their computer. If the attempt to install the software is for official business purposes, the user must have an authorized IT representative update their system for them.

(d) Unless approved in advanced by the IT department, and explicitly noted on the Intranet web site, all content posted on the Intranet is the sole property of the company.

(e) All access to the intranet is limited to internal company users only.

18 Physical and Environmental Security

18.1 Access Security to Offices of the Company

(a) The entrance to the Company shall be secured and monitored at all times (during work hours and thereafter).

(b) The entrance doors to the offices shall be closed and locked at all times; entrance to the areas of the Company shall be through the secretarial counter after identification of the individual, seeking to enter.

(c) Upon completion of the workday, the offices of the Company shall be locked and the alarm of the security company shall be activated.

(d) Monitoring cams shall be placed in order to trace access to the offices of the Company during and after work hours.

18.2 Entrance of Customers/ Visits to the Site of the Company

(a) The entrance of any customer/visits to the offices of the Company shall be through the secretarial counter.

(b) Visitors/customers of the Company shall be accompanied during their entire stay within the area of the Company. The entrance of an external party to the Company shall not be allowed in the absence of continuous coordination and escort.

(c) Waiting of visitors shall be at waiting areas only.

(d) Allowing visitors to enter work areas containing computer infrastructures/server rooms, identified, classified information, should be avoided to the extent necessary, and it should be particularized that the work environment will not include identified information, in order not to expose sensitive information to visitors.

18.3 Security in Work Areas

(a) Workers of the Company ought to pay attention to the presence of unfamiliar individuals, who are wandering at the offices unescorted. In any event of a doubt, the visitor ought to be inquired about his purpose and the Information Security Manager/another manager should be reported to the extent that the response of the visitor is unsatisfactory or if the visitor fails to cooperate.

(b) It should be particularized not to allow unaccompanied visitors to enter the offices of the Company.

(c) The last worker leaving the Company upon completion of the workday is responsible to verify that all doors and windows are locked and that the alarm has been activated.

(d) Keys to the offices and alarm codes should not conveyed to external and temporary parties, such as workers of the cleaning company, couriers or other service providers.

(e) Workers of the Company shall be guided with respect to the information security guidelines, security of the alarm code and the keys to the offices (prohibition of duplication, prohibition to transfer to a third party, reporting of loss, etc).

(f) In the event of a leaving worker or loss of keys to the offices of the Company, an evaluation shall be held in connection with the need to replace the locks and keys at the offices.

18.4 **Clean Table**

(a) Each and every employee is responsible for the information security in his own work environment, the equipment provided to him by the Company and also to any resource of the Company used, held by him or which is accessible to him in his work environment.

(b) Documents and records, which are not temporarily under use, shall be filed and stored in a cabinet or transferred to archives.

(c) Unused documents shall be shredded.

(d) Attention should be given to documents that are exposed during the visit of visitors or external parties to the work environment, while avoiding openly presenting sensitive documents in the work environment.

(e) Keys to cabinets and rooms should not be left unattended.

18.5 **Physical Security Standard in the Company**

(a) Entrances in the area of the Company shall include:

(i) an entrance door with a lock;

(ii) security cams at the entrance to the Company and in the corridors;

(iii) alarm system detectors;

(iv) cabinets that can be locked in the offices where confidential material should be stored;

(v) computer screens shall be positioned in a manner that prevents, to the extent possible, viewing them by individuals who are entering the offices or passing in the corridor;

(vi) a safe installed in the office.

(b) **Physical Security Standard of the Servers Room**

(i) A fire extinguisher suitable for the servers.

(ii) Smoke detectors.

(iii) Volume detector of the alarm system.

(iv) The server room will include equipment, which is part of the IT equipment only.

(v) The presence of authorized parties alone (entrance to authorized only upon passing a worker card or password) shall be allowed to the server room.

(vi) Suppliers and technicians shall be accompanied during their entire stay in the server room/offices of the Company.

(c) **Alarm System**

(i) All areas in the Company should be protected by means of an alarm system.

(ii) The alarm system shall be activated after work hours, by the last worker who leaves the premises.

(iii) The alarm code shall be given only to authorized parties.

(iv) The alarm code shall be periodically replaced.

19 Protection of Physical Information and Digital Media

Physical Information is any information that is in paper form or removable (digital) media form.

19.1 Proper handling and storage of physical information

All physical information that contains any information other than public information must be in a controlled environment if left unattended by an authorized individual. A controlled environment is either an area where access is strictly controlled to essential personnel with a need to be in the area or a locked environment where only authorized individuals have access. General company areas where only employees, contractors, and registered escorted guests have access, but not the public are not considered to be a controlled area. All off-site storage of information must be controlled by an approved storage vendor, and a storage practice that meets the guidelines of IS policy.

19.2 Proper disposal of physical information

Any physical information that contains any information other than public information must be properly disposed of. This includes placing all paper with all confidential content to be shredded or placed in a secured shred bin. All Company's Confidential Information must be shredded prior to being removed from the premises. All removable media that contains any information other than public information must be controlled until the information has been erased or the physical media has been destroyed.

20 Reporting Of Security Incidents

20.1 Employees responsibilities

(a) All suspected information security events must be immediately reported through the proper company internal channels to the IT department. The preferred method is to report suspected incidents using phone or incident system to the IT department.

(b) Company users have the duty to properly report all information security violations and problems to the IT department on a timely basis so that prompt remedial action may be taken.

(c) Unauthorized disclosures of any company's information must be reported to the IT department, which shall notify the involved information owners.

(d) Any attempt to interfere with, prevent, obstruct, or dissuade a staff member in their efforts to report a suspected information security problem or violation is strictly prohibited and is cause for disciplinary action.

(e) Any retaliation against an individual reporting or investigating information security problems or violations is also prohibited and is cause for disciplinary action.

(f) The company shall protect users, who report in good faith, what they believe to be a violation of information security policies. This means that such workers shall not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation.

20.2 Reporting and corrective actions

(a) Whenever evidence clearly shows that a computer has been a victim of a communications crime, the IT department must immediately conduct proper forensics and assist with the reporting processes. The investigation must provide sufficient information so that management can take appropriate action to ensure that (1) such incidents shall not be likely to happen again, and (2) effective security measures have been re-established.

(b) Information describing all reported information security problems and violations must be retained for a period of three (3) years.

21 Computer Viruses, Worms, and Trojan Horses

21.1 **Computer viruses**

(a) A computer virus is an unauthorized program that replicates itself, attaches itself to other programs, and spreads onto various data storage media or across a network. The symptoms of virus infection include slow response times, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failures of computers.

(b) To assure continued uninterrupted service for all information systems, all computers and servers that are attached to the company's network must have an approved virus-screening software enabled on their computers. All Internet gateway servers must have gateway Anti-Virus and Anti-Spam protection running. When new virus signature updates are released for the virus scanning software, the system administrators must force all computers to update their approved virus scanning software upon login. All removable media needs to be scanned for viruses before use in any information system. Disabling the Anti-Virus software can lead to disciplinary actions, including termination.

(c) Although users are responsible for eradicating viruses from their systems whenever they have been detected, they must immediately call the help desk to report the virus. This action allows steps to be promptly taken in order to ensure that no further infection occurs.

(d) Servers must be checked daily for viruses. Such servers and endpoints shall have automatic update of current virus definition files as the source vendor issues them.

21.2 **Worms**

Worms are similar to viruses, but are more dangerous in nature and spread at a much faster rate. Unlike most viruses, where user intervention is involved, worms exploit known vulnerabilities and propagate without any user intervention. Worms do not care for functionality. The fact that the user is connected to the Internet makes him a target for all worms. When a worm is discovered, follow the same procedures as for Computer Viruses eradication in order to stop infection.

21.3 **Trojan horses**

(a) Trojan horses are unauthorized programs that are hidden within authorized programs. To prevent the spread of Trojan horses, do not install any software obtained by un-trusted businesses, for example, unregistered freeware or shareware downloaded from un-trusted Internet sites or from other types of media from un-trusted sources.

(b) If a Trojan horse is detected, follow the same procedures as Computer Viruses.

22 Data backups

22.1 Users must save all of their documents on their shared drive to ensure that the information can be properly backed up.

22.2 All servers and network configurations should be backed up on a daily basis.

22.3 All source code must be backed up by the IT department and stored offsite on a weekly basis.

22.4 **Information Retrieval**

Within the current operation of the Company, the following retrieval activities shall be executed:

(a) partial retrieval - retrieval of folders, files, etc, executed daily and currently on request.

(b) full retrieval - retrieval of server or system, including all their contents, executed only after crash of server/system or once a year, in order to verify the ordered condition of the backup.

23 Monitoring

23.1 The object of monitoring is to discover unauthorized information-processing activities.

23.2 All the actions of users of the information systems of the Company are recorded on the monitoring system, in order to uphold a process of monitoring and documentation upon occurrence of information security incidents or a deviation from the information security policy adopted by the Company

24 Development

24.1 **Development tools and techniques**

(a) Before a new system is developed or acquired, management of the user department(s) must clearly specify the relevant security requirements. Alternatives must be reviewed with the developers or vendors so that an appropriate balance is reached between security and other objectives.

(b) Management must ensure that all software developed and software maintenance activities performed by in-house staff adhere to the company's security policies, standards, procedures, and other system development conventions.

(c) Prior to distributing any developed software or information regarding the software to third parties, the company's developers must first have subjected the software in question to appropriate testing by the R&D product security team.

(d) File naming convention must be employed in order to clearly distinguish between the files used for production purposes and the files used for development and testing purposes by marketing and R&D software teams.

(e) Business application software and development\Labs must be kept strictly separate from the production application software. Development\Labs networks, directories, storage libraries, and physical equipment should be separate from all other company networks. Likewise, testing and quality assurance networks, directories, storage, and physical equipment must be separate from all other company networks and must not share the same network access.

24.2 **Testing of newly developed software**

(a) Unless a written permission is first obtained from the IT department, all software testing for systems designed to handle confidential information must be accomplished exclusively with 'sanitized' production information. Sanitized information is production information that no longer contains specific details that might be valuable, critical, sensitive, or private.

(b) Prior to moving software, which has been developed in-house, to production status, programmers and other technical staff must remove all special access paths so that access may only be obtained via normal secured channels. This means that all backdoors and other short cuts that could be used to compromise the security must be removed. Likewise, all system privileges needed for development efforts, but not required for normal production activities, must be removed.

(c) Business application software development staff shall not be granted access to production information with the exception of the production information relevant to the particular application software, on which they are currently working.

25 Change Control

25.1 Change control policy

(a) All computer and communication systems used for production processing at the company must employ a formal change control procedure, which ensures that only authorized changes are made. This change control procedure must be used for all changes to software, hardware, communication networks, and related procedures.

(b) All security problem-fix software, command scripts, and the like provided by operating system vendors, official computer emergency response teams, and other trusted third parties must go through change management. If the vulnerability needs immediate attention, escalate it to change management review and promptly approve the changes.

26 Third Party Involvement

26.1 Third party software

(a) If procurement of third party software is considered, the management must obtain a written integrity statement from the involved vendor. This statement must provide assurances that the software in question does not contain undocumented features, does not contain hidden mechanisms that could be used to compromise security, and does not require the modification or abandonment of controls found in the operating system on which it runs. Any procurement of software must be approved by Information Security department.

(b) The company should strongly support strict adherence to software vendors' license agreements and copyright holder's notices. If the users make unauthorized copies of software, the users are doing so on their behalf, since the company strictly forbids all such copying. Likewise, the company allows reproduction of copy written material only to the extent legally considered 'fair use' or with the permission of either the author or publisher.

(c) Unless specified by contract, all confidential or proprietary information that has been entrusted to the company by a third party must be protected, as though it is the company's own confidential information.

(d) Exchanges of in-house software or internal information between the company and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange as well as the ways in which the software or information is to be handled and protected. This policy does not cover the release of information designated as public (marketing materials, help wanted postings, etc).

(e) Software licensed by the company may not be sold, copied, or used for personal reasons or gain.

26.2 Restriction of third party access

(a) Inbound VPN access or inbound Internet privileges must not be given to third party vendors unless the IT department determines that these vendors have a legitimate business need for such access. This type of access must be enabled for specific authorized users for the time period required to accomplish the approved task. All approved third party access must be documented and reviewed on a quarterly basis.

(b) All new connection requests between third parties and the company require that the third party and the company's representatives agree to and sign the company's NDA Agreement form. This agreement must be signed by the designated senior manager in the sponsoring organization as well as a representative from the third party, who is

legally empowered to sign on behalf of the third party. All third parties may only be connected to the internal network upon approval of the IT department.

(c) The company reserves the right to update this policy without notice.

27 Management of Business Continuity

27.1 The purpose of the operation is to frustrate disruptions to the operations of the business and to protect critical business procedures from the effect of serious failures of the information systems or disasters, assuring recovery of the necessary resources for continuation of functioning of the Company.

27.2 Within the framework of management service, resources of the Company that are essential on emergency shall be defined, as well as defining a recovery program upon occurrence of a disaster, pursuant to the continuance of the rendering a reliable and efficient service to customers of the Company.

27.3 As part of business continuity plan of the company examined two main scenarios:

(a) disabling company server activity - in this case the Company's operations will be stopped until an establishing the backup server recovery. The server will be set up within 48 hours of downtime while restoring backup data exchange to be set up in a server;

(b) disabling company's physical site due to fire / terrorist activity - In this case the company's activity will be able from employees houses / externally. Within three days the company will return to full operations from its offices or from alternatively site after purchasing appropriate computer equipment.

28 Adjustment

28.1 **Adjustment to the requirements by law and regulatory requirements**

(a) The management of the Company applies the laws, standards and additional regulatory respondents, applying to the Company.

(b) The CEO of the Company is responsible to verify that all the workers of the Company are aware of the laws, regulations and procedures derived wherefrom.

(c) Identification of laws and regulations on information issues:

(i) rights of intellectual property;

(ii) legal evidence and records of the Company;

(iii) right to privacy;

(iv) business and economic confidentiality;

(v) prevention of abuse of information-processing possibilities.

(d) By adopting this information security system, the management of the Company fulfills and implements that required by laws and standards, in aspects of information security, which it is interested and obligated to meet:

(i) information security management standards - Israeli Standard ISO 27001;

(ii) The Computers Law, 1995;

(iii) Privacy Protection Law, 1981;

(iv) Copyrights Law, 1911;

(v) working according to overseas regulatory requirements.

(e) At least once a year, a 'management survey' on issues of information quality and security is held in order to scan and examine the degree of adjustment of the policy that was adopted to the actual occurrences

(f) Internal tests are executed in the organization at least once a year, in order to examine the degree of adjustment of the assistance and procedures to the organizational security policy.

(g) Within the framework of the surveys and the adjustment tests, the degree of strength of the infrastructure of the information systems against hazards and malicious software will be examined.

29 Controls and auditing

29.1 All procedures shall have controls designated to assure the proper implementation of the procedure.

29.2 Audit trails shall be implemented in the various systems and shall be regularly monitored and controlled.

30 Responsibility

The Information Security Officer is responsible to apply and maintain the Policy.

31 Applicability

31.1 The Policy shall apply to all Company employees, subsidiaries, outsourcers and all external entities wishing to connect to Company Systems.

31.2 Information security procedures, derived from this Policy, shall be published to the proper factors, in accordance with their content.

31.3 Deviation from Policy shall require the authorization of the Information security Manager.