



Policy on Assessing the Independence of Directors

Vection Technologies Ltd ACN 614 814 041 (Company)

An independent director is a director who is free of any interest, position, association or relationship that might influence, or reasonably be perceived to influence, in a material respect his or her capacity to bring an independent judgment to bear on issues before the Board and to act in the best interests of the Company and its security holders generally.

It is the Board's policy that in determining a director's independence, the Board considers the factors relevant to assessing the independence of a director as set out in Box 2.3 of the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations (3rd edition). Examples of interests, positions, associations and relationships that might cause doubts about the independence of a director include if the director:

- (a) is, or has been, employed in an executive capacity by the Company or any of its child entities and there has not been a period of at least three years between ceasing such employment and serving on the Board;
- (b) is, or has within the last three years been, a partner, director or senior employee of a provider of material professional services to the Company or any of its child entities;
- (c) is, or has been within the last three years, in a material business relationship (eg as a supplier or customer) with the Company or any of its child entities, or an officer of, or otherwise associated with, someone with such a relationship;
- (d) is a substantial security holder¹ of the Company or an officer of, or otherwise associated with, a substantial security holder of the Company;
- (e) has a material contractual relationship with the Company or any of its child entities other than as a director;
- (f) has close family ties with any person who falls within any of the categories described above; or
- (g) has been a director of the Company for such a period that his or her independence may have been compromised.

In each case, the materiality of the interest, position, association or relationship needs to be assessed to determine whether it might interfere, or might reasonably be seen to interfere, with the director's capacity to bring an independent judgment to bear on issues before the Board and to act in the best interests of the Company and its security holders generally.

¹ For this purpose a "substantial security holder" is a person with a substantial holding as defined in section 9 of the Corporations Act. As at the date of this policy this equals 5%.
Vection Technologies Ltd (ASX:VR1) ACN: 614 814 041

Asia Pacific

Address: Suite 1, 437 Roberts Road
Subiaco WA 6008, Australia
Phone: +618 6380 2555

Europe

Address: Via Isonzo 61
40033 Casalecchio di Reno (BO), Italy

Media Enquiries

AUpres@vection.com.au
EUpres@vection.com.au



Policy and Procedure for Selection and (Re)Appointment of Directors

Vection Technologies Ltd ACN 614 814 041 (Company)

New directors

It is the policy of the Board that in determining candidates for the Board, the following process shall occur:

- (a) The Nomination Committee evaluates the mix of skills, experience, expertise and diversity of the existing Board. In particular, the Nomination Committee (or equivalent) is to identify the particular skills and diversity that will best increase the Board's effectiveness. Consideration is also given to the balance of independent directors on the Board. Regard must also be had to the Company's *Diversity Policy* in identifying appropriate candidates.
- (b) The Nomination Committee will identify potential candidates by seeking applications from suitably qualified individuals; and/or placing advertisements in appropriate media; and/or engaging external consultants that will present diverse candidates.
- (c) The Nomination Committee interviews selected candidates.
- (d) A potential candidate is considered with reference to their skills and expertise in relation to other Board members. The Nomination Committee will also have regard to the other matters identified in this *Policy and Procedure for Selection and Re(Appointment) of Directors* as relevant when identifying and considering candidates for the Board.
- (e) If relevant, the Nomination Committee recommends an appropriate candidate for appointment to the Board. The Nomination Committee must undertake appropriate checks before recommending an appropriate candidate for appointment to the Board. These should include checks as to the person's character, experience, education, criminal record and bankruptcy history.
- (f) Any appointment made by the Board is subject to ratification by shareholders at the Company's next annual general meeting.
- (g) The Company must enter into a written agreement with each director appointed to the Board setting out the terms of their appointment.

Board renewal

The Board recognises that Board renewal is critical to performance and the impact of Board tenure on succession planning. Re-appointment of directors is not automatic. The Company must hold an election of directors each year. Under the Company's Constitution, a director of the Company must not hold office (without re-election) past the third annual general meeting following the director's appointment or three years, whichever is longer. However, a director appointed to fill a casual vacancy or as an addition to the board must not hold office (without re-election) past the next annual general meeting of the entity. This rule does not apply to the Managing Director.

Size and composition of the Board

The Board should be structured in such a way that it has a proper understanding of, and competence to deal with, the current and emerging issues of the business and encourages enhanced performance of the Company.

Reference is made to the Company's size and operations as they evolve from time to time.



Commitment to the Board

Non-executive directors must provide to the Nomination Committee (or equivalent), prior to their appointment or re-election, details of their other commitments and an indication of the time involved in carrying out those other commitments.

All directors should consider the number and nature of their directorships and calls on their time from other commitments. Prior to appointment, or being submitted for re-election non-executive directors are required to specifically acknowledge to the Company that they will have sufficient time to fulfil their responsibilities as a director.

Informing shareholders

Shareholders will be informed of the names of candidates submitted for election as directors. So that shareholders can make an informed decision on whether or not to elect or re-elect a candidate as a director, the following information will be supplied to shareholders:

- (a) biographical details, including their relevant qualifications and experience and the skills they bring to the Board;
- (b) details of any other material directorships currently held by the candidate;
- (c) if the candidate is standing for election as a director for the first time:
 - (i) *any material adverse information revealed by the checks the Company has performed about the candidate;*
 - (ii) *details of any interest, position, association or relationship that might influence, or reasonably be perceived to influence, in a material respect his or her capacity to bring an independent judgment to bear on issues before the Board and to act in the best interests of the Company and its security holders generally; and*
 - (iii) *if the Board considers that the candidate will, if elected, qualify as an independent director, a statement to that effect;*
- (d) if the candidate is standing for re-election as a director:
 - (i) *the term of office currently served by the director; and*
 - (ii) *if the Board considers the director to be an independent director; a statement to that effect; and*
- (e) a statement by the Board as to whether it supports the election or re-election of the proposed candidate.



Whistleblower Policy

Vection Technologies Ltd ACN 614 814 041 (Company)

Report and Investigation Officer: Derek Hall

1 Purpose

Directors, officers and employees of the Company are expected to observe high standards of business and personal ethics in the conduct of their duties and responsibilities as set out in the Company's *Code of Conduct*. All directors, officers and employees of the Company must conduct themselves with integrity, honesty and fairness in all business practices and observe the rule and spirit of the legal and regulatory environment in which the Company operates.

The purpose of this Whistleblower Policy is to encourage the reporting of violations (or suspected violations) of the Company's *Code of Conduct* and provide effective protection from victimisation or dismissal to those reporting by implementing systems for confidentiality and report handling.

2 Reporting responsibility

It is the responsibility of all directors, officers and employees to comply with the Company's *Code of Conduct* and report violations or suspected violations in accordance with this policy.

3 No retaliation

No director, officer or employee who in good faith reports a violation under this policy shall suffer detriment, either actual or threatened, harassment, retaliation or adverse employment or engagement consequence. If a director, officer or employee retaliates against someone who has reported a violation in good faith they will be subject to disciplinary action, which may include termination of your employment or engagement with the Company.

4 Reporting violations

This policy is intended to encourage and enable directors, officers and employees and others to raise serious concerns within the Company.

In most cases, you should approach your supervisor first as they may be in the best position to address a concern.

If you are not comfortable speaking to your supervisor or not satisfied with your supervisor's response, you are encouraged to speak with anyone in management whom you are comfortable in approaching.

Supervisors and managers are required to report suspected violations of the Company's *Code of Conduct* to the Report and Investigation Officer, who has specific and exclusive responsibility to investigate all reported violations.

5 Report and Investigation Officer

The Report and Investigation Officer is responsible for investigating and resolving all reported complaints and allegations concerning violations of the Company's *Code of Conduct*.

At their discretion, the Report and Investigation Officer will advise the Chair and Managing Director and/or the Audit Committee or its equivalent.

The Report and Investigation Officer has direct access to the Audit and Risk Committee and, is required to report to the Audit and Risk Committee at least annually on compliance activity.



If any person is not comfortable speaking with the Report and Investigation Officer on a particular matter, or if they are unavailable and the matter is urgent, they should contact the Chair or another member of the Board.

6 Accounting and auditing matters

The Audit and Risk Committee will address concerns raised in relation to corporate accounting practices, internal controls or auditing. The Report and Investigation Officer is responsible for notifying the Audit and Risk Committee of any such complaint and must work with the committee to resolve the matter.

7 Acting in good faith

Anyone filing a complaint concerning a violation or suspected violation of the Company's *Code of Conduct* must act in good faith and have reasonable grounds for believing the information disclosed indicates a violation of the Company's *Code of Conduct*. It is a serious matter to make allegations that prove to be unsubstantiated, or are made maliciously or known to be false and any person doing so may be subject to disciplinary action including termination.

8 Confidentiality

Reports of violations or suspected violations will be kept confidential and may only be disclosed to ASIC, APRA, a member of the Australian Federal Police or to someone else with the consent of the discloser to the extent possible, consistent with the need to conduct an adequate investigation.

9 Handling of reported violations

The Report and Investigation Officer will notify the person who reported the alleged violation and acknowledge receipt of the report within 5 business days. All reports will be promptly investigated and, if warranted, appropriate corrective action will be taken. In conducting investigations, the Report and Investigation Officer must ensure they observe the confidentiality obligations and in particular must not disclose the information reported, the identity of the person making the disclosure or any information that is likely to lead to the identification of the person making the disclosure.



Process for Performance Evaluations

Vection Technologies Ltd ACN 614 814 041 (Company)

Board, Board committees and individual directors

The Chair evaluates the performance of the Board by way of an informal round-table discussion with all directors and through questionnaires completed by each director.

The Chair reviews the performance of the committees of the Board by way of an information round-table discussion with all directors and through questionnaires completed by each director who is a member of the committee being evaluated.

Individual director's performance evaluations are completed by the Chair. The Chair meets with each individual director and reviews questionnaires completed by each director.

Chair

The Senior Independent Director is responsible for evaluating the performance of the Chair after having canvassed the views of the other directors via the questionnaires completed by each director.

Managing Director

The Managing Director's performance evaluation is conducted by the Chair. The Chair conducts a performance evaluation of the Managing Director by way of meeting with the Managing Director and with an informal round-table discussion with all directors, and by reference to the Managing Director's key performance indicators which are set by the Nomination and Remuneration Committee.

Senior executives

The Managing Director (and in their absence the Board) reviews the performance of the senior executives. The Managing Director conducts a performance evaluation of the senior executives by way of on-going information monitoring throughout each financial year and at an annual formal interview.



Privacy and Data Protection Policy

The Following Privacy Policy Contains Details on:

- What personal data we collect
- What client data we collect
- How and Why we collect this data
- Once data is collected, how it is used
- How data is retained or destroyed respectively
- How we store and secure your personal data
- Any third parties that may have access to this data
- Our policy on the use of cookies
- How individual clients may control any aspects of the data we have collected on them personally.

Who We Are:

Our Company Vection Technologies Ltd ("Vection", "us", "we", or "our") operates vection.com.au (the "Site") and Vection back office services ("Services"). This policy outlines our procedures regarding the collection, use and disclosure of Personal Information and or Data we receive from users of the Site and users of our Services.

Our Commitment:

At Vection, we are committed to protecting the privacy and security of any personally identifiable information provided to us. This includes information that can be linked to a specific individual, such as a name, address, contact number, contact email, Tax File Numbers etc.

This privacy policy explains how we handle and protect your personally identifiable information in accordance with commonly accepted privacy principles.

This policy was last revised on 31 May 2018.

As needs change, we reserve the right to modify or amend this policy at any time and for any reason. Any material changes to this privacy policy will be posted prior to their implementation. If you would like to ask a question about this policy, you can send it by email or post:

Email: support@vection.com.au

Post: Privacy Officer
Suite 1, 437 Roberts Road
Subiaco, WA 6008

Responsibilities:

All Vection staff are responsible for ensuring that data they produce, collect, or use is properly classified, stored and protected and destroyed in accordance with this policy. The Directors are responsible for assigning data custodians within the Company to facilitate this policy. The data custodian must:

- Be familiar with this policy in particular document retention and destruction;
- Develop the department's data management procedures and practices, consistent with this policy;
- Educate staff within the company in understanding sound data management practices;
- Restrict access to Protected and Sensitive data and information; and
- Coordinate the destruction of data.



Data custodians should develop and maintain data inventory lists; classify data as Protected, Sensitive, or Public; and properly set a schedule and mode of retaining and destroying data in accordance with applicable Commonwealth state and international regulations. Data should not be retained beyond the period that it is needed for business processes or business continuity.

The following 8 points outline your personal legal rights surrounding the storage and handling of your personal data:

Individuals have the right to;

1. The right to be informed – all organisations must be completely transparent in how they are using personal data (personal data may include data such as a work email and work mobile if they are specific to an individual).
2. The right of access - individuals will have the right to know exactly what information is held about them and how it is processed.
3. The right of rectification - individuals will be entitled to have personal data rectified if it is inaccurate or incomplete.
4. The right to erasure - also known as 'the right to be forgotten', this refers to an individual's right to having their personal data deleted or removed without the need for a specific reason as to why they wish to discontinue.
5. The right to restrict processing - an individual's right to block or suppress processing of their personal data.
6. The right to data portability - this allows individuals to retain and reuse their personal data for their own purpose.
7. The right to object - in certain circumstances, individuals are entitled to object to their personal data being used. This includes, if a company uses personal data for the purpose of direct marketing, scientific and historical research, or for the performance of a task in the public interest.
8. Rights of automated decision making and profiling - the GDPR has put in place safeguards to protect individuals against the risk that a potentially damaging decision is made without human intervention. For example, individuals can choose not to be the subject of a decision where the consequence has a legal bearing on them, or is based on automated processing

Personal Information:

While using our Site, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to - your name, email and phone number ("Personal Information").

We use your Personal Information for purposes such as subscribing to Vection news alerts or requesting further information from Vection. By using the Site, you agree to the collection and use of information in accordance with this policy.

Client Information:

While using our Services, you may provide us with sensitive information ("Sensitive Data"). This Sensitive Data will be used for the purpose proscribed to us by you – and for no other purpose.

Upon request, following completion of the Services, we will see to secure destruction of the Sensitive Data as per our Data Disposal procedures.

All data covered by the scope of this policy will be classified as **Protected, Sensitive, or Public**.



Types of Data – sensitive, protected and public:

Protected data is paper or electronic data that contains personally identifiable information concerning any individual; is regulated by local, state, Commonwealth or applicable international privacy regulations or any voluntary industry standards; or best practices concerning protection of personally identifiable information that the Vection chooses to follow. Any paper or electronic data that contain this information must be classified as Protected data by default.

Examples of Protected data may include, but are not limited to:

- Social Security Numbers, names, addresses, email addresses, telephone numbers
- Credit Card and Debit Card Details
- Bank Account numbers and Tax File Numbers
- Drivers licence/ state identification cards: details and numbers

Sensitive data is any paper or electronic data that is not classified as Protected data which Vection would not distribute to the general public. Any data is classified as Sensitive unless the company gives a more specific classification.

Examples of Sensitive data may include, but are not limited to:

- Client advising records
- Client property transaction records
- Client account data
- Client data for data entry purposes
- Financial application files
- Budgets
- Salary information
- General Client information

Public data is any paper or electronic data that Vection is comfortable distributing to the general public.

Examples of the types of data included as Public are:

- Press releases
- Vection web site content

Information Use:

We use your Personal Information to service your requests and may share your personal information within the company where someone may “need to know” that information. We may also disclose your personal information to third parties including the authorities if there is a regulatory or legal requirement to do so.

Security:

To maintain the confidentiality of your Personal Information and Sensitive Data, we use leading security technology and procedures that are regularly reviewed and updated. This technology spans our international offices.

Our systems are configured with industry standard data encryption and firewall technology. When you send personally identifiable information to us over the Internet, your data is protected by Secure Socket Layer (SSL) technology to provide for safe transmission. The protection of data transmission is indicated by the presence of a lock or key symbol in your Internet browser.

The security of your Personal Information and Sensitive Data is important to us but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use



commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

Data Disposal:

PROCEDURES

All computer desktops, laptops, hard drives, and portable media must be processed through Management for proper disposal. Paper and hard copy records shall be disposed of in a secure manner as specified by the archiving and destruction policy. The Directors shall ensure procedures exist and are followed that:

Address the evaluation and final disposition of Sensitive Data, hardware, or electronic media regardless of media format or type.

Specify a process for making Sensitive Data unusable and inaccessible. These procedures should specify the use of technology (e.g. software, special hardware, etc.) or physical destruction mechanisms to ensure sensitive information is unusable, inaccessible, and unable to be reconstructed.

Authorise personnel to dispose of Sensitive Data or equipment. Such procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed. Approved disposal methods include:

Physical Print Media shall be disposed of by one (or a combination) of the following methods:

Shredding - Media shall be shredded using [LEP] issued cross-cut shredders.

Shredding Bins - Disposal shall be performed using locked bins located on-site using a licensed and bonded information disposal contractor.

Incineration – Materials are physically destroyed using licensed and bonded information disposal contractor.

Electronic Media (physical disks, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the methods:

Overwriting Magnetic Media – Overwriting uses a program to write binary data sector by sector onto the media that requires sanitisation

Degaussing – Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state

Physical Destruction – implies complete destruction of media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated

IT documentation, hardware, and storage that have been used to process, store, or transmit Confidential Information or PII shall not be released into general surplus until it has been sanitized and all stored information has been cleared using one of the above methods.

Cloud Data Storage shall be disposed of according to the following procedure:

Upon commencement of Services, a dedicated Sensitive Data folder will be set up by the relevant Data custodian. Only those staff members who are performing the Services will be provided access and access will be monitored by the Data custodian.

Upon completion of Services, the Data custodian will:

1. remove access from all users from the Sensitive Data folder;
2. delete the Sensitive Data from the cloud data server;
3. delete the emptied folder and confirm deletion.



In all instances, data provided by a client to Vection will be removed from the Vection environment and deleted within 30 days of either termination of an agreement or the completion of an engagement.

Log Data and Cookies:

Like many site operators, we collect information that your browser sends whenever you visit our Site ("Log Data"). This Log Data is non-personally-identifiable and may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics. In addition, we may use third party services such as Google Analytics that collect, monitor and analyse this.

Cookies are files with small amount of data, which may include an anonymous unique identifier. Cookies are sent to your browser from a web site and stored on your computer's hard drive. Like many sites, we use "cookies" to collect information. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Site.

Regulations:

Regulations applicable to this policy include, but are not limited to:

- GDPR (general data protection regulation) requirements.
- APP (Australian Privacy Protection) requirements.

More information on the recent GDPR guidelines –

<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>

Questions about this policy and Your Personal Data

Questions regarding this policy and/or the procedures contained in it should be addressed to Vection's privacy officer. Furthermore, if you personally would like to:

- request access to any information that Vection has stored about you
- correct any personal data that Vection has stored about you
- Delete any information that Vection has stored about you

You are well within your rights to contact the Vection privacy officer to do so.

Contact Details:

Email: support@vection.com.au

Post: Privacy Officer
Suite 1, 437 Roberts Road
Subiaco, WA 6008

About Vection (ASX:VR1):

Vection is a multinational software company that makes 3D, Virtual Reality (VR) & Augmented Reality (AR) software services for the engineering, manufacturing, architecture, construction & education industries. Vection operates on an Enterprise business model based on bespoke fees and on a Software as a Service (SaaS) business model based on recurring subscription revenue.

www.vection.com.au