NSW Workplace Surveillance Policy

1 Purpose

1.1 [Insert company name] (the **Company**) wishes to ensure the safety of employees, horse welfare and protect and secure property and assets. For these reasons, the Company has workplace surveillance practices in place.

1.2 Under the *Workplace Surveillance Act 2005* (NSW) (the **Act**), the Company has the right to conduct workplace surveillance, which may include camera surveillance, computer surveillance and/or tracking surveillance.

1.3 Surveillance implemented by the Company shall occur in accordance with the provisions of the Act and this policy.

2 Objective

2.1 This Policy aims to ensure that the Company complies with the requirements of the Act and to provide detail regarding the workplace surveillance that may be carried out at the Company.

3 Scope

3.1 This Policy applies to:

(a) all Company staff (full-time, part-time and casual), and other relevant persons performing work at the direction of the Company (**Staff**); and

(b) all of the Company's workplaces and other places where Staff may be working or representing the Company, for example, a customer, client or supplier's premises (**Workplace**).

4 Purpose of surveillance

4.1 The purpose of workplace surveillance at the Company is:

(a) monitor horse and staff welfare;

(b) to monitor Staff's use of computers, email, the internet and communication devices ensure security of the training establishment;

(c) to monitor Staff's compliance with conduct requirements and other company policies and procedures;

(d) to monitor potential exposure to legal liability or breaches of security or confidentiality; and

(e) for the purpose of investigating allegations of misconduct or to provide materials to external investigative authorities lawfully investigating possible criminal conduct.

4.2 Employees, contractors, volunteers, visitors, clients, or any other persons shall not be permitted to tamper with, or alter, the operation of any surveillance device without the prior written approval of the Company

5 Notification

5.1 This policy, and its subsequent distribution to all current and new Staff, is intended to meet the Company's obligations of notification of workplace surveillance of employees, pursuant to the Act.

5.2 Existing Staff of the Company shall be notified of existing surveillance activities through the dissemination of this Policy. Implementation will begin 14 days after the adoption of this Policy.

5.3 Staff yet to commence with the Company will receive written notification before they commence their employment, through the issuance of this Policy.

5.4 This notification of surveillance indicates:

(a) the kind of surveillance to be carried out (camera, computer or tracking);

(b) how the surveillance will be carried out;

(c) when the surveillance will start;

(d) whether the surveillance will be continuous or intermittent; and

(e) whether the surveillance will be for a specified period or ongoing.

5.5 Under the Act, Staff who are not working at their usual workplace will not be notified of camera surveillance at any alternate workplaces where they may work from time to time, including but not limited to surveillance that may occur at racetrack locations.

5.6 Any new or upgraded software, camera, computer or other surveillance instrument will not require prior staff notification unless the new or upgraded software, camera, computer or other surveillance instrument is to be used for a purpose not specified in this policy.

6 Manner of Surveillance

6.1 The Company will use overt cameras, email filters, internet monitoring software and devices, and tracking devices, and any other similar surveillance methods permitted by the relevant legislation, deemed appropriate, from time to time.

6.2 Audits of surveillance information may be conducted by the Company and the results will be provided to managers and directors.

7 Computer, internet, email and communication device surveillance

7.1 Computer surveillance may be conducted via computer, internet and/or email monitoring systems to monitor communication devices, including mobile phones, tablets,

digital organisers and any other digital communication devices of a like nature, provided during employment by the Company.

7.2 Devices and equipment which the Company monitors includes workstations, computers, laptops, servers, mobile devices including mobile phones, email and network services, printers, network connected devices, and connections to internet services supplied by the Company (including fixed, Wi-Fi and 3G/4G).

7.3 Surveillance can monitor and record the following details:

(a) emails sent and/or received by Staff;

(b) internet sites accessed by Staff;

(c) software applications accessed by Staff;

(d) other input or output from Company computers;

(e) text messages or other forms of digital communication, e.g. videos, photos, images sent and/or received by Staff using mobile phones supplied by the Company; and

(f) the use, input and output of communication devices as noted above.

7.4 The Company may use computer surveillance to access and monitor Staff's use of Company software applications, email and internet systems in the following ways:

(a) monitoring email server performance and retaining logs, backups and archives of emails sent and received through the server. Even where the user has deleted an email, the Company may still retain archived and/or backup copies of the email;

(b) retaining logs, backups and archives of all software applications access, internet access, and network usage; and

(c) viewing real-time computer and software application use.

7.5 All messages generated on or handled by our internet/email facility, including back-up copies, are considered to be property of the Company.

7.6 Staff's emails are not routinely read or monitored. However, emails are records of the Company and should be managed accordingly and will be accessible in that context.

7.7 While individual computer, internet and email usage is not routinely monitored, unusual or high-volume activities may warrant more detailed examination.

7.8 Use of the Company's computers and associated systems is governed by the Company's IT, Internet and Social Media Policy.

7.9 Computer surveillance records will only be used as outlined under the Act and referred to in clause 9.1 of this Policy.

8 Camera Surveillance

8.1 Cameras which monitor and record visual images will be used to monitor activities within Company Premises on a continuous and ongoing basis. The Company may require designated areas to be under surveillance for the following reasons:

(a) to protect the safety of Company Staff and clients/visitors;

(b) to ensure the security of Company property and assets;

(c) for operations requirements; and

(d) to investigate accidents and/or incidents.

8.2 Cameras will be placed in locations which are visible, or known, to people in the Company Premises. Workplace facilities and areas that are subject to camera surveillance will have appropriate signage displayed notifying Staff and the public that they may be under surveillance, in accordance with the Act.

8.3 Camera surveillance will not be carried out in change rooms, toilets, showers or other bathing locations.

8.4 Where camera surveillance is proposed in remote work sites, the Company will notify relevant employees before commencing camera surveillance.

8.5 The Company reserves the right to introduce additional camera surveillance at any of their locations, to monitor security and provide employee and public safety. The introduction of additional cameras is the responsibility of the Company's leadership team and will be operated in accordance with this Policy. Where the Company intends to install new camera surveillance devices, employees working in the designated area or areas will be notified in accordance with this policy and relevant legislation.

8.6 The Company will erect visible signs informing people who enter or leave the Company Premises that camera surveillance is being carried out.

8.7 Information or knowledge secured or obtained as a result of camera surveillance under this policy will only be used as outlined under the Act and referred to in clause 8.7 of this Policy.

9 Use and disclosure of surveillance records

9.1 The Company will ensure that any surveillance records made as a result of workplace surveillance are not used or disclosed, except in accordance with the Act where that use or disclosure is:

(a) as part of investigations for disciplinary purposes and as evidence during any disciplinary proceedings or legal proceedings;

(b) for a legitimate purpose related to the employment of employees of the employer or the legitimate business activities or functions of the employer, or in connection with the enforcement of the Company's legal rights;

(c) for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings;

(d) in connection with suspected corruption, illegal activity, maladministration, misuse or theft of the Company information or resources; or

(e) in instances wherein the employer reasonably believes there is an imminent threat of serious violence to persons or of substantial damage to property.

9.2 Information recorded or obtained by surveillance:

(a) will only be used in accordance with this policy, indexed, stored and destroyed;

(b) may only be viewed by the Company, police, and any person or entity for the purposes of analysis, decoding or presentation of data;

(c) which is required as evidence will be properly copied and recorded prior to being provided to third parties for the purposes of investigation or enforcement of proceedings or legal issues;

(d) will not be made available to the media for commercial or entertainment purposes; and

(e) will be disposed of securely.

9.3 If surveillance information is required at any other time by a manager or director, the manager or director must gain authority from the Company to access that information for a specific purpose and an approved period.

10 Prohibitions

10.1 Individual Staff are prohibited from undertaking surveillance in their workplace. Where it is necessary to undertake new or additional workplace surveillance it will be in accordance with this Policy and approved by the relevant Managers.

10.2 Cameras in mobile telephones, either personally owned or supplied by the Company are not to be used to record images of any persons on Company premises without their knowledge and consent.

11 Breach

11.1 Any breach of this policy may result in the Company counselling, or taking disciplinary action, against an employee, which may include the provision of warnings and termination of employment.

12 Definitions

12.1 Under the Act, "**surveillance**" means surveillance of Staff by any of the following means:

(a) "**Camera surveillance**", meaning surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place;

(b) **"Computer surveillance"**, meaning surveillance by means of software or other equipment that monitors or records the information input or output, or other use of a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites); and

(c) "**Tracking surveillance**", meaning surveillance by means of an electronic device, the **primary** purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device).

14 Agreement

14.1 This policy constitutes all notice as required by the Act and any other legislation.

14.2 By receiving this policy, you are deemed to have been given sufficient notice and your continued attendance at the Company's Workplaces constitutes acceptance of all forms of surveillance outlined in this policy.