RSPCT BASKETBALL TECHNOLOGIES LTD. SECURITY INSTRUCTIONS FOR CLIENTS

1. Overview

RSPCT Basketball Technologies Ltd. (the "**Company**" or "**RSPCT**") is committed to protect its clients' information from illegal and/or damaging actions by third parties, either knowingly or unknowingly.

At RSPCT, we critically depend on continued client confidence, and would like to assure that such confidence shall be lost due to misappropriate use of the System or its equipment.

RSPCT System Equipment (as defined below) is under the control of Client's staff members, in the courts, offices, during practices etc. In addition, it's Client's staff members who deals with information gathered by the System and System's deliverables and outcomes.

It is Client's responsibility to apply high standard of security measures, to familiar its staff members with those measure, and to conduct their activities accordingly. The following are only baselines to security measures required to be applied while using RSPCT System.

2. The System and It's Equipment

2.1 The "System" means – A system for real-time, accurate tracking of basketball shots in a basketball court. The System includes:

2.1.1 "**System Equipment**" which includes the "**Basket Kit**" components: sensor, computer, cables, mounts. Each Basket Kit is installed per one (1) basket in court, meaning System Equipment include all Basket Kits installed at Client's facilities.

2.1.2 "**Software**" – the Software is installed on the applicable component per each Basket Kit and will be used by Client on Company's computer. Client may also access the Software from its own devices.

2.1.3 "**Application(s)**" - To be used on Client's devices such as smartphone, tablet or laptop\desktop, which provides outcomes of the System, whether in print or electronic data as tracking shooting of player(s) (as time, shot origin, shot arc, shot grade, shot result), summary of practice sessions and more.

2.2 The "**Services**" means the use of the Software and Application(s) as a SAAS (software as a service) Solution.

3. Client Points of Contact with RSPCT SYSTEM

3.1 These guidelines apply to Client's personnel and anyone of Client's behalf, who may have access to Client's facilities where the System Equipment is installed and/or stored and to Client personnel members who has access to the Applications from personal device(s) and/or Client's device(s) and/or System Equipment (computer). The following are example for the major point contacts with RSPCT System Equipment and Software:

3.1.1 Trained Personnel Members: Client's employees, who has been trained by Company's staff with respect to the installation and the use the System;

3.1.2 Permitted Users: Client's employees who has been registered by Client as users of the Software, including providing them username and password.

3.1.3 Client person of contact – Client's employee who has been defined in the Agreement between RSPCT and Client as contact person.

3.1.4 Client's staff members and other persons in the court and/or Client's facilities with access to the System Equipment itself.

4. Security Guidelines

4.1 General

4.1.1 For the purpose of these guidelines it is hereby clarified that the System processing information that may be considered as proprietary, confidential and personal, whether to RSPCT or Client (as applicable) (the "**Data**").

4.1.2 Therefore, that Data is protected, secured and handled according to several international, federal and local laws. It is utmost important to RSPCT to keep this information safe together with Client's efforts.

4.1.3 Per Client's equipment, Client shall handle, process, record, delete, share and handle the Data in accordance with the international, federal and local laws, specifically with respect (but not limited) to privacy, confidentiality, data security, data destruction, consumer protection, advertising, electronic mail, and any other related or similar laws (acts / rules / regulations etc.) and shall apply commercially accepted industry best practices to apply such laws.

4.1.4 Client shall only share Data to the extent it's permitted by the applicable law and the Agreement between the Company and Client.

4.1.5 All prints of Data / outcomes / results / analyses provided by the Services shall be

handled and marked as "Confidential" and "Private".

4.1.6 Client shall handle and operate the System Equipment with its Trained Personnel Members and Permitted Users only. Such staff members should be carefully selected with restricted access as Client shall instruct, in order to keep the System Equipment and the Data safe and aligned with the applicable law.

4.1.7 Client must assure that each of its employee and/or staff members may only access, use or share Data to the extent it is authorized and necessary to fulfill his/her assigned job duties.

4.1.8 Client shall inform its staff members regarding these guidelines and make sure they follow them.

4.1.9 Client has a responsibility to promptly report any theft, loss or unauthorized disclosure of Data. In addition, Client's Contact Person shall contact RSPCT regarding any (and all) security matters with respect to the System, including informing RSPCT to block access of Client's employee / former employee, loosing/ theft of System Equipment (or part of them), passwords violations etc.

4.1.10 Moreover, it is under Client responsibility to handle, by the applicable Client's officer, all access control administration activities (including, but not limited to sensitivity classification category relevant to the Data), monitor the security of Client personnel regarding the System, and creating guidelines regarding keeping the applicable System Equipment locked and secured when it is not under use.

4.1.11 When a Permitted User or any other staff member with password to the System leaves Client, it is the responsibility of Client to promptly inform RSPCT that the privileges associated with such Permitted User's / staff member's USER ID and password must be revoked. USER IDs are specific to individuals, and must not be reassigned to, or used by, others.

4.2 Password

4.2.1 Client is responsible to determine a policy for a password mechanism. The following should be included in such policy: password should be "hard to guess", should be changed every 6 months and must not be shared with other Client's staff members and/or other third parties.

4.2.2 Per each Permitted User, RSPCT shall use the USER ID created by Client's system only and which shall be provided to RSPCT by Client ("**User ID**"). Such USER ID shall be linked to the password of such USER ID. This will ensure that only the applicable Permitted user is able to access the relevant information of the USER ID. It is clarified that Permitted Users are responsible for all activity that takes place with their USER ID and password or other authentication mechanism.

4.2.3 Password must be changed immediately if there is a suspicious that the password has

been discovered or used by another person. Please notify RSPCT immediately whether there is a suspicious of compromising any of access control mechanisms.

4.3 RSPCT Computer / Client's Device / Staff Member's Personal Device

4.3.1 Client is aware that shot tracking information recorded by the Software and displayed on the computer, which is part of the Basket Kit (the "Computer"), shall be stored on such Computer for the following 48 hours as of the time it was recorded. Therefore, Client must restrict any access to the Computer (and Application(s)) to staff members with a "need to know basis".

4.3.2 Computer must be, at all times, marked as "Confidential" and locked in a secured place while not in used.

4.3.3 Client must create guidelines and restrictions per the installation and users of the Application(s) on personal device(s).

4.3.4 Per all of Client's devices and/or personal devices used by Client's staff members, Client shall apply industry standard protocols, technics and tools to detect and prevent malfunctions and Illicit Codes which may penetrate the Software and/ or the System equipment. “Illicit Code” means viruses, malware, worms, time bombs, Trojan Horses, backdoors, trapdoors, and any other harmful or malicious code.

5. Security Breach

5.1 With respect to any security breach or suspicious of security breach, which was caused due to Client's failure to protect and secure the Data in accordance with the applicable law and these guidelines – Client shall be the sole responsible to conducts, on its own expense, investigation of such breach, to notice any such actual or suspected breach as required by the applicable law and to follow the applicable laws regarding such breach. In such notice, Client shall not refere to RSPCT as liable per such breach. In this event, RSPCT shall cooperate with Client's investigation, but shall not be liable to the results of such breach, including any costs, damages and/or legal fees.