Raise 365 Cyber Incident Response Plan (IRP)

1. Purpose. The purpose of this cyber incident response plan ("IRP") is to provide a structured and systematic incident response process for all information security incidents (as defined in Section 4, Information Security Incident) that affect any information technology ("IT") systems, network, or data of Raise 365 Developments, LLC ("COMPANY"), including COMPANY's data held or IT services provided by third-party vendors or other service providers.

1.1. Specifically, COMPANY intends for this IRP to:

(a) Define COMPANY's cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.

(b) Assist COMPANY and any applicable third parties in quickly and efficiently responding to and recovering from different levels of Information Security Incidents.

(c) Mitigate or minimize the effects of any Information Security Incident on COMPANY, its customers/clients, employees, and others.

(d) Help COMPANY consistently document the actions it takes in response to Information Security Incidents.

(e) Reduce overall risk exposure for COMPANY.

1.2. COMPANY developed and maintains this IRP as may be required by applicable laws and regulations, including state, federal and international, additionally the General Data Protection Regulation of the European Union ("GDPR").

2. Scope. This IRP applies to all COMPANY business groups, its employees, contractors, officers, and directors, and COMPANY's IT systems, network, data, and any computer systems or networks connected to COMPANY's network or software. This IRP used should be in conjunction with COMPANY Cyber Security Policy ("CSP") and related Privacy Documents as defined in the CSP. Defined terms used in this IRP shall have the meanings ascribed to them in the CSP and related Data Security and Privacy Documents. In the event of a conflict between this IRP and the CSP or other COMPANY Data Security and Privacy Documents, this IRP shall control and be interpreted accordingly.

3. Accountability. COMPANY has designated our Chief Technology Officer to implement and maintain this IRP.

3.1. Chief Technology Officer Duties. Among other information security duties, as defined in the CSP, the Chief Technology Officer shall be responsible for:

(a) Implementing this IRP.

(b) Identifying the incident response team ("IRT") and any appropriate sub-teams to address specific Information Security Incidents, or categories of Information Security Incidents (see Section 5, Incident Response Team).

(c) Coordinating IRT activities, including developing, maintaining, and following appropriate procedures to respond to and document identified Information Security Incidents (see Section 6, Incident Response Procedures).

(d) Conducting post-incident reviews to gather feedback on Information Security Incident response procedures and address any identified gaps in security measures (see Section 6.7, Post-Incident Review).

(e) Providing training and conducting periodic exercises to promote employee and stakeholder preparedness and awareness of this IRP (see Section 7, Plan Training and Testing).

(f) Reviewing this IRP at least annually, or whenever there is a material change in COMPANY's business practices that may reasonably affect its cyber incident response procedures (see Section 8, Plan Review).

3.2. Enforcement. Violations of or actions contrary to this IRP may result in disciplinary action, in accordance with COMPANY's information security policies.

4. "Information Security Incident." Information security incident means an actual or reasonably suspected (a) loss or theft of Personal Data or other Confidential Information; (b) unauthorized use, disclosure, acquisition of or access to, or other unauthorized processing of Personal Data or other Confidential Information that reasonably may compromise the privacy or confidentiality, integrity, or availability of Personal Data or other Confidential Information; or (c) unauthorized access to or use of, inability to access, loss or theft of, or malicious infection of COMPANY's IT systems or third party systems that reasonably may compromise the privacy or confidentiality, integrity, or availability of Personal Data or other Confidential Information or COMPANY's operating environment or services.

5. Incident Response Team. IRT is a predetermined group of COMPANY employees and resources responsible for responding to Information Security Incidents.

5.1. Role. The IRT provides timely, organized, informed, and effective response to Information Security Incidents to (a) avoid loss of or damage to COMPANY's IT systems, network, and data; (b) minimize economic, reputational, or other harms to COMPANY and its customers/clients, employees, and partners; and (c) manage litigation, enforcement, and other risks.

5.2. Authority. Through this IRP, COMPANY authorizes the IRT, under the direction of the Chief Technology Officer, to take reasonable and appropriate steps necessary to mitigate and resolve information security incidents, in accordance with the escalation and notification procedures defined in

this IRP.

5.3. Responsibilities. The IRT is responsible for:

(a) Addressing Information Security Incidents in a timely manner, according to this IRP.

(b) Managing internal and external communications regarding Information Security Incidents.

(c) Reporting its findings to management and to applicable authorities, as appropriate.

(d) Reprioritizing other work responsibilities to permit a timely response to Information Security Incidents on notification.

5.4. IRT Roster. The IRT consists of a core team, led by the Chief Technology Officer, with representatives from key COMPANY groups and stakeholders. The Chief Technology Officer will publish the current IRT roster from time to time.

(a) Sub-Teams and Additional Resources. The Chief Technology Officer assigns and coordinates the IRT for any specific Information Security Incident according to incident characteristics and COMPANY needs. The Chief Technology Officer may:

(i) Identify and maintain IRT sub-teams to address specific Information Security Incidents, or categories of Information Security Incidents.

(ii) Call on external individuals, including vendor, service provider, or other resources, to participate on specific-event IRTs, as necessary. A list of these external resources shall be maintained by the Chief Technology Officer.

6. Incident Response Procedures. COMPANY shall develop, maintain, and follow incident response procedures as defined in this Section 6 to respond to and document identified Information Security Incidents.

COMPANY recognizes that following initial escalation, the Information Security Incident response process is often interactive and the steps defined in Sections 6.3, Investigation and Analysis; 6.4, Containment, Remediation, and Recovery; 6.5, Evidence Preservation; and 6.6, Communications and Notification may overlap or the IRT may revisit prior steps to respond appropriately to a specific Information Security Incident.

COMPANY may, from time to time, approve and make available more specific procedures for certain types of Information Security Incidents. Those additional procedures and checklists are extensions to this IRP.

6.1. Detection and Discovery. COMPANY shall develop, implement, and maintain procedures to detect, discover, and assess potential Information Security Incidents through automated means and individual reports.

(a) Automated Detection. COMPANY shall develop, implement, and maintain automated detection means and other technical safeguards.

(b) Reports from Employees or Other Internal Sources. Employees, or others authorized to access COMPANY's IT systems, network, or data, shall immediately report any actual or suspected Information Security Incident to the Chief Technology Officer. Individuals should report any Information Security Incident they discover or suspect immediately and must not engage in their own investigation or other activities unless authorized.

(c) Reports from External Sources. External sources who claim to have information regarding an actual or alleged Information Security Incident should be directed to the Chief Technology Officer. Employees who receive emails or other communications from external sources regarding Information Security Incidents that may affect COMPANY or others, security vulnerabilities, or related issues shall immediately report those communications to the Chief Technology Officer and shall not interact with the source unless authorized.

(d) Assessing Potential Incidents. COMPANY shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. COMPANY shall document each identified Information Security Incident, with initial details.

6.2. Escalation. Following identification of an Information Security Incident, the Chief Technology Officer shall perform an initial risk-based assessment and determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to COMPANY and its customers/clients, employees, or others.

Based on the initial assessment, the Chief Technology Officer shall:

(a) IRT Activation. Notify and activate the IRT, or a sub-team, including any necessary external resources (see Section 5.4, IRT Roster).

(b) IRT Expectations. Set expectations for IRT member replay and engagement.

(c) Initial Notifications. Notify (if necessary) organizational leadership and any applicable business partners or service providers, and law enforcement or other authorities (see Section 6.6, Communications and Notifications).

6.3. Investigation and Analysis. On activation, the IRT shall collaborate to investigate each identified Information Security Incident, analyze its affects, and formulate an appropriate response plan to contain, remediate, and recover from the incident.

The IRT shall document its investigation and analysis for each identified Information Security Incident.

6.4. Containment, Remediation, and Recovery. Next, the IRT shall direct execution of the response plan it formulates according to its incident investigation and analysis to contain, remediate, and recover from each identified Information Security Incident, using appropriate internal and external resources (see Section 6.3, Investigation and Analysis).

6.5. Evidence Preservation. The IRT shall direct appropriate internal or external resources to capture and preserve evidence related to each identified Information Security Incident during investigation, analysis, and response activities (see Sections 6.3, Investigation and Analysis and 6.4, Containment, Remediation, and Recovery). The IRT shall seek counsel's advice, as needed, to establish appropriate evidence handling and preservation procedures and reasonably identify and protect evidence for specific Information Security Incidents.

6.6. Communications and Notifications. For each identified Information Security Incident, the IRT shall determine and direct appropriate internal and external communications and any required notifications. Only the Chief Technology Officer may authorize Information Security Incident related communications or notifications. The IRT shall seek counsel's advice, as needed, to review communications and notifications targets, content, and protocols.

(a) Internal Communications. The IRT shall prepare and distribute any internal communications it deems appropriate to the characteristics and circumstances of each identified Information Security Incident.

(i) Organizational Leadership. The IRT shall alert organizational leadership to the incident and explain its potential impact on COMPANY, its customers/clients, employees, and others as details become available.

(ii) General Awareness and Resources. As appropriate, the IRT shall explain the incident to COMPANY's employees and other stakeholders, and provide them with resources to appropriately direct questions from customers/clients, media, or others.

(b) External Communications. Working with legal counsel, the IRT shall prepare and distribute any external communications it deems appropriate to the characteristics and circumstances of each identified Information Security Incident. A Template Data Security Incident Notice Letter is attached as Appendix 1 to this IRP.

(i) Public Statements. If COMPANY determines that external statements are necessary, the Chief Technology Officer shall provide consistent, reliable information to the media and public regarding the incident using COMPANY's website, press releases, or other means. All such communications must be approved by legal counsel.

(ii) Law Enforcement. The Chief Technology Officer, working with legal counsel, shall report criminal activity or threats to applicable authorities, as COMPANY deems appropriate.

(c) Notifications. While the IRT may choose to authorize discretionary communications, certain laws, regulations, and contractual commitments may require COMPANY to notify various parties of some information security incidents. If applicable to a specific Information Security Incident, as required, the IRT shall:

(i) Authorities. Notify applicable regulators, law enforcement, or other authorities within seventy-two (72) hours of any breach of Personal Data that poses a risk of harm.

(ii) Affected Individuals. If an applicable breach of Personal Data occurs, prepare and distribute notifications to affected individuals as soon as reasonably possible and without undue delay.

(iii) Notify customers/clients or business partners according to current agreements.

6.7. Post-Incident Review. At a time reasonably following each identified Information Security Incident, the Chief Technology Officer shall reconvene the IRT, others who participated in response to the incident, and affected work group representatives, as appropriate, as a post-incident review team to assess the incident and COMPANY's response.

(a) Review Considerations. The post-incident review team shall consider COMPANY's effectiveness in detecting and responding to the incident and identify any gaps or opportunities for improvement. The post-incident review team shall also seek to identify one or more root causes for the incident and, according to risk, shall recommend appropriate actions to minimize the risks of recurrence.

(b) Report. The post-incident review team shall document its findings.

(c) Follow-Up Actions. The Chief Technology Officer shall monitor and coordinate completion of any follow-up actions identified by the post-incident review team, including communicating its recommendations to and seeking necessary authorization or support from COMPANY leadership.

7. Plan Training and Testing.

7.1. Training. The Chief Technology Officer shall develop, maintain, and deliver training regarding this IRP that periodically, but at least annually:

(a) Informs all employees, and others who have access to COMPANY's IT systems, network, or data, about the IRP and how to recognize and report potential Information Security Incidents.

(b) Educates IRT members on their duties and expectations for responding to Information Security Incidents.

The Chief Technology Officer may choose to include training on this IRP in other information security training activities as defined in the CSP.

7.2. Testing. The Chief Technology Officer shall coordinate exercises to test this IRP periodically. The Chief Technology Officer shall document test results, lessons learned, and feedback and address them in plan reviews (see Section 8, Plan Review).

8. Plan Review. COMPANY will review this IRP at least annually, or whenever there is a material change in COMPANY's business practices that may reasonably affect its cyber incident response procedures. Plan reviews will also include feedback collected from post-incident reviews and training and testing exercises. The Chief Technology Officer must approve any changes to this IRP and is responsible for communicating changes to affected parties.

9. Effective Date. This IRP is effective as of April 26, 2024.