Raise 365 CYBER SECURITY POLICY

1. PURPOSE

Raise 365 Developments, LLC ("Raise 365" or the "Company") is committed to achieving a targeted level of protection from internal and external cyber security threats, and accordingly, will implement ongoing governance, policies, and practices which address the following objectives:

- Ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach.
- Ensure compliance with all applicable laws, regulations, and Raise 365's policies, controls, standards and guidelines.
- Comply with requirements for confidentiality, privacy, integrity, and availability for Raise 365's employees, contractors, vendors, and other users.
- Establish controls for protecting Raise 365's information and information systems against theft, abuse, and other forms of harm or loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of, and knowledge about information security.
- Ensure the protection of Raise 365's data and information assets.
- Ensure the availability and reliability of the network infrastructure, systems and the services.
- Ensure that external service providers are made aware of, and comply with, Raise 365's information security needs and requirements and continuously assess whether they maintain an acceptable cyber security posture.
- Balance the need for the above with the investment and policy constraints required to achieve an appropriate level of protection while maintaining business agility.

2. SCOPE

This policy applies to all permanent and temporary employees of Raise 365 and all subsidiaries, and to directors, independent contractors, consultants, vendors, suppliers, agents, and other users of Raise 365's mobile application software and information technology resources (together referred to as "users") wherever they may be located. The policy is structured in the following categories:

A. Leadership and governance
B. Human factors
C. Information risk management
D. Business continuity
E. Operations technology; and,
F. Legal and compliance

Any breach of this policy is a serious offence and will result in the consideration of appropriate sanctions up to and including termination of employment, contract or legal action.

3. DETAILS

A. Leadership and Governance

Cyber security is a strategic business matter for Raise 365. It is not a technical consideration. The assessment and management of Cyber Risk is integrated into our Company policies for the Company as a whole. Accordingly:

- The development and promulgation of a cyber security plan at the Company is the responsibility of the Chief Technology Officer.
- The implementation of the cyber security plan is the responsibility of operations and functional leadership who are accountable for the results.
- Oversight of the effectiveness of the cyber security plan is the responsibility of the General Counsel.
- Cyber risk should be reflected in reports and updates to operations management, senior management as well as other stakeholders of the Company at least quarterly.
- Cyber risk should be considered by all levels of leadership where changes to business processes, including but not limited to, the information and technology environment.

B. Human Factors

Authorized use: Raise 365 provides access to information technology to users, including the internal environment, the internet and social media, where relevant and useful for their roles within or for Raise 365. Raise 365 prohibits use of IT resources for any purpose other than business, unless otherwise stated in this policy. All users must behave honestly with vigilance, respect the intended business use of technologies and comply with software licenses, property rights, user agreements, confidentiality, and legal rights. Users must comply with Raise 365's policies, and all applicable law when using Raise 365's information technology resources, including without limitation privacy and intellectual property laws.

Raise 365 systems must not be used for the creation or distribution of any material considered inappropriate, offensive, threatening, abusive, defamatory, unlawful, sexually explicit, sexist, racist, discriminatory, embarrassing, fraudulent or disrespectful to others or that could potentially breach any corresponding software license agreements. Raise 365 restricts all users from using its software or other technologies to perform any task contrary to the law or knowingly accessing websites with content that is illegal, obscene, hateful, defamatory, indecent, objectionable, or inappropriate.

To maintain the integrity of Raise 365's corporate image and reputation and to prevent the unauthorized or inadvertent disclosure of sensitive, confidential or personal information, employees must exercise caution and care when using any system, service or technology platform, both internal and external, including email or third party services, such as Cloud-based and social media. Personally identifiable information, which is any data that could identify a specific individual, should not be transmitted via email or shared using any other service (with the exception of site level or corporate HR or legal groups) without approval by the appropriate site or corporate HR group. For clarity, a description of personally identifiable information is provided in **Appendix I**. Employees must also exercise caution against suspicious messages and technologies, which are often intended to bait a user into a malicious cyber event.

Passwords: Users are responsible for utilizing effective passwords and for keeping those passwords secret and secure. Employees must not appropriate, use or disclose someone else's login or password without prior authorization by the employee's supervisor or Human Resources. In addition, employees should ensure that the function of retaining passwords by company computers is disabled. The Chief Technology Officer will support the mechanisms that evaluate the strength of passwords and define the password change frequency for every type of applications, services and devices supported by the Company, along with other mechanisms to strengthen the way users identify themselves when accessing Raise 365's IT resources, such as multifactor authentication. A guide to the development of acceptably effective passwords and the required frequency of change is provided in **Appendix II**.

Active Directory Accounts: Internal accounts used by Raise 365 personnel must have a unique User ID and password, and cannot be used by or shared with anyone other than the for whom it is intended. Personnel external to Raise 365 (i.e. consultants and/or contractors) should also be provided with unique user IDs and passwords, and follow the same internal controls relating to the granting and/or revoking of access as internal Raise 365 accounts.

Contractors, vendors and/or consultants must ensure all accounts/passwords assigned to them will be stored in a secure password vault.

The use of shared accounts (i.e. more than one person using a single User ID and password) is not permitted under any circumstance.

Active Directory constitutes the official corporate directory of users and it must reflect up to date information, including but not limited to, user's full name, department or functional area the user is associated with, direct reports, phone numbers, organizational position or role, etc. It is the responsibility of every department or functional area lead to ensure the information is current by advising Human Resources of any change. Corporate IT will provide the mechanism to enable this update process.

***Confidentiality*:** Raise 365 prohibits the release of confidential information to any third party, or use of confidential information, except as required in the performance of Raise 365-related work approved by the employee's supervisor and in accordance with the terms of the applicable confidentiality agreement.

Privacy: Users should have no expectation of personal privacy in anything they create, store, send or receive by e-mail or when using any corporate application if they use equipment (e.g. mobile device, computers) owned or provided by Raise 365. The nature of Raise 365's business requires effective monitoring of activities on Raise 365's network, including the conduct of users. Raise 365 reserves the right to review and collect all information contained in e-mails, whether or not stored solely in personal folders on the computer operated by the user, and in all equipment owned or provided by Raise 365.

Ownership**:** Data and User's work and work products belong to Raise 365, including all messages, sent or received regardless of the device or application used to produce, send or receive it.

Security**:** Used unwisely, the Internet can be a source of security problems that can do significant damage to the Company. Users must:

- Apply best practices to prevent any form of computer virus, Trojan, spyware or other malware from being into the company's environment. A list of actions to prevent this from occurring which every employee must be aware is provided in **Appendix III**. While this list is not exhaustive, it is illustrative of the burden of care that every employee agrees to accept in helping ensure the security of the Company and its IT environment.

- Only access websites, applications or systems for which they have authorization, either within the company or outside it.
- Only use approved services for the uploading or sharing of company data.

Awareness, Communication and Training:

New Employees: To mitigate the risk of unintentional disclosure of confidential information by employees, Company will refer newly onboarded employees to this policy and will require formal acknowledgement that it has been read, is understood and will be applied.

New and Existing Employees: To mitigate the risk of unintentional disclosure of confidential information by employees, cyber security training and awareness sessions will be provided as an integral part of employee onboarding and ongoing employee development. In addition, acknowledgement of this policy, that it is understood and that the employee agrees to apply it will be included in the annual sign off along with the code of conduct.

Departures and/or changes in employment status: Upon a change in status, including promotion, transfer or termination of employment the applicable Company department is accountable for ensuring that the local IT leader is advised so that the employee's network and physical access privileges are modified as appropriate in a timely manner.

Third Parties: Third parties, vendors, suppliers, partners, contractors, service providers, or customers with connectivity to Raise 365's internal network or access to Raise 365's data must comply with this Policy and the policy governing system access by third parties.

C. Information Risk Management

The Company will develop, maintain and periodically review for appropriate updates risk appetite statements that:

- Articulate its position with respect to cyber risk.
- Specifically address the degree of protection (as measured by a "cyber maturity index" or some other appropriate benchmark) that we are targeting and how we will measure it.

The Company will develop, maintain and periodically update as required, an inventory of major types of information and systems on the basis of criticality to the business. This list, on a priority basis, will be used to formally assess the degree of cyber protection that the company has, the target degree of protection as well as the plans that are in place to achieve the desired level as appropriate. The target level will reflect the nature of the information or application as well as the risk appetite defined above.

D. Business Continuity

The Chief Technology Officer is responsible for the development and promulgation of standards and guidelines for acceptable IT related business continuity and disaster recovery plans.

E. Operations Technology

Data, applications, and networks, new software and IT equipment: To prevent the deployment of software and IT equipment that could compromise the security of the entire information technology infrastructure, the Chief Technology Officer will establish standards for the development, acquisition, or installation and approval of all new software and major equipment purchases. No software should be installed on Company-owned devices unless approved by the Chief Technology Officer. Raise 365 installs only properly authorized and licensed software and prohibits any installation or use of unauthorized, unlicensed or illegally-copied software.

Change Management: To protect from changes that could compromise Raise 365's operations, the Chief Technology Officer will enforce standards for the approval and deployment of changes to the information technology infrastructure and environment as well as the implementation of any new applications of any type. These standards, require, amongst other provisions, that all changes be appropriately governed and managed – and must be tested, documented, with cyber, business, technical and legal risk areas considered, and have user acceptance documented before being installed in the production environment. The approved deployment plan must include rollback and contingency procedures.

Viruses and Malware: To defend the company from computer viruses and malware, all computers and devices connecting to Raise 365's infrastructure must be approved devices and have the standard, authorized anti virus and malware protection software installed. It is responsibility of the Chief Technology Officer to keep this software updated and of users to report to the Chief Technology Officer any sign of infection. To further enhance security, personal email is not to be accessed, either through the web browser or applications, on Company laptops or computers. It is acceptable to sync tablets and mobile phones to personal email accounts as these devices do not access the company network.

Incident management: To promptly respond to threats, users are expected to communicate information security incidents to the Chief Technology Officer in accordance with the incident response breach policy. Security incidents include any violation of this security policy that compromises corporate data independently of ownership of the device. The Chief Technology Officer is responsible for the channels and procedures that guarantee that security incidents are identified, contained, investigated, and remedied.

F. Legal and Compliance

Raise 365 will regularly assess developments within the company and in the environment, and ensure the promulgation of corporate wide policies for:

- Cyber security management
- Management of third party’s access to company networks
- Other policies as required to ensure minimum standards of care are taken by the organization to protect against cyber threat.

Cyber risk will be monitored through the Company’s cyber security software and audited through the Company’s Internal audit programs and be included in the report communicated to the executive team quarterly.

All material contracts should be reviewed by legal counsel as a matter of course and to ensure that the potential cyber risk assumed or created as a result is understood by management.

All contracts for the provision of cyber related services to the company should be reviewed by legal counsel to ensure that management has the understanding of residual risks for purposes of making relevant business decisions.

Issue Date:	January 1, 2023	**Authorized By:**
Review:	Annually	CEO&CTO
Revised Date:	April 26, 2024	

Appendix I - Personally Identifiable Information

Personally identifiable information (PII) is any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources. It includes information that is linked or linkable to an individual, such as medical, educational, financial and employment information. Examples of data elements that can identify an individual include name, fingerprints or other biometric (including genetic) data, email address, telephone number or social security number. Safeguarding company-held PII (and other sensitive information) is the responsibility of each and every member of the workforce. Regardless of your role, you should know what PII is and your responsibility in ensuring its protection.

Although society has always relied on personal identifiers, defining and protecting PII has recently become much more important as a component of personal privacy, now that advances in computing and communications technology, including the internet, has made it easier to collect and process vast amounts of information. The protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed

PII can also be exploited by criminals to steal a person's identity or commit other crimes. According to FBI statistics, identity theft continues to be one of the fastest growing crimes and can cause both financial and emotional damage to its victims. Due to this threat, many governments have enacted legislation to limit the distribution of personal information.

The following list contains examples of information that may be considered PII.

- Name, such as full name, maiden name, mother‘s maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver‘s license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well- defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Sometimes, one or two pieces of information can be combined with other information to compromise someone’s identity, even if the individual pieces of information seem harmless.

Appendix II - Tips for creating a strong password

Passwords provide the first line of defense against unauthorized access to your computer. The stronger your password, the more protected your computer will be from hackers and malicious software. You should make sure you have strong passwords for all accounts on your computer. If you're using a corporate network, your network administrator might require you to use a strong password**.**

What makes a password strong (or weak)?

A strong password:

- Is at least eight characters long.
- Does not contain your user name, real name, or company name.
- Does not contain a complete word.
- Is significantly different from previous passwords.
- Contains characters from each of the following four categories:

Character category	**Examples**
Uppercase letters	A, B, C
Lowercase letters	a, b, c
Numbers	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

A password might meet all the criteria above and still be a weak password. For example, Hello2U! meets all the criteria for a strong password listed above, but is still weak because it contains a complete word. H3ll0 2 U! is a stronger alternative because it replaces some of the letters in the complete word with numbers and also includes spaces.

Help yourself remember your strong password by following these tips:

- Create an acronym from an easy-to-remember piece of information. For example, pick a phrase that is meaningful to you, such as **My son's birthday is 13 December, 2005**. Using that phrase as your guide, you might use **Msbi13/Dec,5** for your password.
- Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase. For example, **My son's birthday is 13 December, 2005** could become **Mi$un's Brthd8iz 13125** (it's OK to use spaces in your password
- Relate your password to a favorite hobby or sport. For example, **I love to play badminton** could become **ILuv2PlayB@dm1nt()n**.

Appendix III - List of best practices to prevent any form of computer virus, Trojan, spyware or other malware infection

- Do not open emails from unknown senders.
- Don’t click on any links within emails that seem suspicious or from unknown senders.
- Don’t install any software on company issued computers without prior approval from IT Dept.
- Only open websites that you know. Never randomly click a link as it may direct you to a malicious website or trick you to download an infected file or program.
- When using USB flash drives, thumb drives or any other removable drives, make sure you scan them using your security software. Best practice is to ask IT dept. to scan if you’re not too sure.
- Limit the amount of information that is published on the internet about yourself or about Raise 365. This can be used for social engineering.
- Report any suspicious computer activity to IT Dept. right away.
- Educate yourself on the protection systems that are installed on your computer and to check if it is up to date or any alerts.
- Never leave your computer unattended while outside the company offices where anyone could plug in a USB device. As a best practice always lock your computer session before leaving your computer-unattended