Radix Technologies LTD.

Security Practices and Measures Overview

[Last Updated: March 2024]

Radix Technologies Ltd. ("**Radix**", "**Company**" or "**we**") is committed to provide transparency regarding the security measures and policies which it has implemented in order to secure and protect its customers data, with emphasize towards personal data and personal identifying information as defined under applicable data protection law (together "**Personal Data**").

As part of our data protection compliance process, we have implemented technical, physical and administrative security measures to protect Personal Data. This document outlines those technical and organizational practices.

The Company security practices, and management system are aligned with company's certification under iso 27001 security standard, and include the following:

- **Control Environment, Management Involvement and Overall Security Management**
  Radix's data security practices are anchored in a robust control environment, defined by a strong awareness and attitude towards internal controls from its management under the supervision of the board. Authority and responsibility are clearly defined and communicated through organizational structures and policies. Management routinely assesses risks and compliance, emphasizing security and confidentiality. Human resources policies strengthen this framework, focusing on hiring competent personnel, providing necessary training, and ensuring compliance with security policies. The company's management actively supports security-related development, allocating adequate funding and resources as outlined in the global Radix security plan.
- **Risk Assessment and Mitigation**
  Having a pre-defined clear and detailed risk assessment strategy is integral to Radix data security framework, focusing on identifying, analyzing, and mitigating risks that could impact its objectives and its services. This involves a thorough evaluation of information assets, threats, and vulnerabilities, both internal and external. The company employs a formal risk management program, continuously addressing information security risks through a variety of treatment options like acceptance, avoidance, mitigation, and transfer. Key decisions on risk treatment are documented and approved annually by management (as part of the iso 27001 certification), ensuring that risk mitigation is effectively integrated into the company's overall risk management strategy.
- **Penetration Testing**
  An external web application penetration test is conducted on a regular basis. Critical and High issues are investigated and resolved in a timely manner. High/Critical issues are investigated and dealt with in accordance with Radix SDLC process or by any necessary means. A re-test is performed to verify the remediation of the relevant issues.

- **Access Control, User, and Permissions Management**
  Radix implements stringent access control and user permissions management to ensure the security of its information assets. Access is strictly limited to what is necessary for an employee's or contractor's role, governed by group-based permissions aligned with job descriptions and responsibilities. This access is regularly reviewed and approved quarterly by management. Radix enforces robust password standards, including requirements for character complexity and password history. Additional security measures include controlled system resource access, especially for higher privilege accounts, and enforced security settings on company laptops like encryption, and remote wipe capabilities. The company also has a prompt revocation process for user accounts upon job termination, further safeguarding against unauthorized access. Any remote access to Radix resources and data assets is regulated behind MFA mechanisms, in order to enforce and ensure stringent security measures.
- **Production System Access**
  Radix maintains rigorous access controls within its production environment to safeguard system integrity and data security. Access to the production environment is heavily restricted, with two-factor authentication, ensuring that only authorized personnel gain entry. For backup access, alterations and deletions are strictly controlled, accessible only to authorized users and again protected by two-factor authentication. The same level of security applies to source control and sensitive database access, ensuring robust protection against unauthorized changes or data breaches.
- **Physical Access and Visitors**
  Physical access to the offices is restricted to authorized personnel using a designated key-code or key. The premises are further protected through an alarm system and a 24/7 manned receptionist or guard in the entrance to the building. Visitors are required to be always accompanied by a Radix employee during their stay. Employees encountering an unfamiliar or suspicious person wandering around the office are expected to ask them politely about the nature of their business and if necessary, accompany them to their host. Visitors are not allowed to access or connect to Radix company’s network or equipment.
- **Data Center Security**
  Radix's data center security is reinforced through its reliance on AWS's global infrastructure, which encompasses facilities, networks, hardware, and operational software. This infrastructure adheres to stringent security best practices and complies with various security standards and regulations, including iso 27001, 27017 and 27018 and Soc2.
- **Application Security and SDLC**
  Radix's application security framework includes rigorous penetration testing to prevent unauthorized access to confidential information, with regular external tests and prompt resolution of critical issues. They also implement robust vulnerability management, conducting regular internal scans and quarterly production network scans, ensuring timely remediation of high-risk vulnerabilities, especially in source code as part of the SDLC.

- **Logical Security**
  Radix employs a managed configuration system for server and patch management, maintaining hardened security settings across devices. This is complemented by endpoint protection on employee devices and restricted software installation, ensuring a secure and controlled application environment.
- **Job Control**
  All of the Company's employees are required to execute an employment agreement which includes confidentiality provisions as well as applicable data protection provisions binding them to comply with the Company's policies, in particular the computer security policy. In addition, employees undergo a screening process applicable per regional law. In the event of a breach of an employee's obligation or non-compliance with the Company's policies, the Company includes repercussions to ensure compliance with the policies all according to the Company's Employee's Manual.
- **Employee Awareness and Training**
  Radix places a strong emphasis on security awareness and training for all employees, recognizing the importance of understanding their information security responsibilities. This is achieved through the communication of security policies and guidelines, underpinned by the Radix security awareness program. A mandatory annual security awareness training program is in place for all employees. This training covers critical areas such as common security risks and threats, compliance with regulations, understanding of the Acceptable Use Policy, information security practices, data protection and customer privacy, laptop security, and awareness of social engineering tactics including fraud and phishing.
- **Encryption**
  Radix employs robust data encryption strategies to protect both data in transit and data at rest, enhancing its overall data security posture. For data in transit, the company ensures secure communication between its customers and company assets through the use of HTTPS with TLS 1.2 authenticated certificates. All restricted information assets, such as databases and backups containing customer data, are encrypted at least at the disk level. Moreover, customer content stored at rest is automatically encrypted using multiple encryption mechanisms. This process involves splitting data into chunks, each encrypted with a unique data encryption key. These keys are stored alongside the data but are encrypted with key encryption keys. These key encryption keys are managed within the providers' central key management services, which are redundant and globally distributed. This layered encryption approach ensures a high level of security for stored data, mitigating risks and enhancing customer trust.
- **Transfer Control**
  Except for transfer data to our business partners, The Company does not transfer any Personal Data outside of the Company's cloud servers. All transfer of Personal Data between the client side and the Company's servers is protected using encryption and safeguards, as well as encryption of the Personal Data prior to the transfer of any Personal Data. The Company's servers are protected by industry standards. Furthermore, the destruction of Personal Data following termination of the engagement is included within the contract between the parties. In addition, to the extent applicable, the Company's business partners execute an applicable Data Processing Agreement, all in accordance with applicable laws.

- **Data Retention**
  Personal Data is retained for as long as needed to provide the services or as required under applicable laws. Individuals may request data deletion; however, this request is not absolute and is limited, all as detailed in the Company Privacy Policy.
- **Vendor Security and Management**
  Prior to the Company's engagement with third party contractors, the Company reviews such third party's security policies to ensure it complies with the Company's standard for data security protection. Third party contractors may solely access the Personal Data as explicitly instructed by the Company. Any relevant supplier is required to sign a DPA or an NDA in accordance with its processing operations on behalf of the Company. The Company reviews its vendors on an annual basis as part of its iso 27001 certification.