KRAKEN CODING
Healthcare Application Development

Privacy, Security and Documentation Policy

KRAKEN CODING SECURITY GROUP
Last Updated 11/03/2024

Privacy, Security and Documentation Policy

Table of Contents

Kraken Coding Privacy Commitment

Kraken Coding commits to provide appropriate and necessary protections and safeguards to ensure the legitimate use, proper disclosure, and minimal contact of any Personal Information, which, for Kraken Coding, encompasses the legal and regulatory definitions of personal data to include any and all information or data (regardless of format) that (i) identifies or can be used to identify, contact or locate an individual, or (ii) that relates to an individual, whose identity can be either directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of any attributes or status of such individual.

Kraken Coding uses a framework of controls based on ISO, NIST and Australian Privacy Law requirements to:

(1) identify the specific purposes for which we may need to collect, use, or disclose Personal Information,

(2) operationalise protections surrounding Personal Information relating to the privacy rights of individuals while ensuring availability for proper and authorized uses and disclosures,

(3) implement safeguards to secure the confidentiality, integrity, and availability of Personal Information in our environments,

(4) address education and awareness through a comprehensive staff training initiative and

(5) respond promptly to any actual or suspected threats or vulnerabilities affecting

Personal Information.

Our privacy program is led by our Director and Data Protection Officer:

- *Name:* *John Shanks*
- *Email:* *john@krakencoding.com*
- *Phone:* *0466357927*
- *Post:* *PO Box 40431 Casuarina NT 0811*

This policy highlights more specifics of our data protection, privacy, and security practices as they pertain to the Kraken Coding processes, products, and services.

Purposes

Any collection, use, or disclosure (or processing) of Personal Information by Kraken Coding is directly related to the purposes for which the information was originally gathered either by Kraken Coding (or on behalf of Kraken Coding) or by a customer of Kraken Coding supporting the legitimate interests pursued by the appropriate party, which may be a personal information processor, covered business or data controller. Those interests may include:

- Support and advisory activities relating to Kraken Coding processes, products, or services, which will include necessary contract and response information for the issue reported (individual requesting support) and any personal information relating to the specific support information.
- Managed Services and hosting activities where Kraken Coding provides solutions tocustomers and their end users and participants, which would include not only any personal information relevant to the delivered solution (and any supporting environments), but the personal information of individual end users to the extent supported through the solution and shared with Kraken Coding.
- Issue investigation and resolution relating to personal information or personal data, including patient records – where this cannot be performed by the local organisation support or without access to the personal information, such as when a user has completed an action in error and wants to undo the transaction or rectify the result or a user is unable to complete an action due to application error.
- Implementation of a new system or an upgrade to existing system, to include testing that the system is functioning correctly, because behaviours may be specific to existing data rather than new data added.

- Data migration services, either during implementation for the population of a new live environment with data from a legacy system or for a major upgrade where database version compatibility is an issue.
- Interface testing where the external system does not have a test environment to which to connect.
- Support of interfaces between clinical systems and disparate operational support systems with patient data.
- Support of national reporting – e.g. Commissioning Data Sets.
- Sales and marketing activities related to Kraken Coding products and services and the contact information as well as interactions with individuals, including any online activities, attendance at Kraken Coding' events, and direct inquiries from individuals.
- Internal functions addressing personnel, facilities, and technology resources, such as payroll and email systems.

Technical and Organisational Measures

Privacy Protections

Kraken Coding incorporates and harmonizes the requirements of privacy and data protection legislation and regulation related to the collection, use, and disclosure of Personal Information through the implementation of policies and procedures, training on support and operational practices, and controls and measures focused on the relevant protections.

- **Data Protection Officer – John Shanks:** To oversee the accountability of Kraken Coding in delivering on its promises for data protection..
- **Fair Processing:** To assist our customers in carrying out their mission and objectives through our delivery, support, and maintenance of information systems and processes that collect, use, and disclose Personal Information.
- **Lawful Purposes:** To ensure our collection, use, and disclosure of Personal Information links to our support of our customers as data controllers.
  Kraken Coding uses contracts and procedures with our customers to links any processing of Personal Information to the purposes relevant to the services or support we provide.

- **Minimum Necessary:** To make sure that Kraken Coding collection, use, and disclosure of Personal Information is adequate, relevant and not excessive.

  Kraken Coding examines incoming data for Personal Information to ensure receipt only that information relevant and related to the services or support delivered.

- **Data Integrity:** To address the accuracy of Personal Information that is collected, used, and disclosed.

  Kraken Coding employs its technology to make certain that data, including Personal Information, maintains integrity through external vendor processing while providing our services or support.

- **Limited Retention:** To maintain Personal Information for only as long as appropriate and necessary to address the needs of our customers.

  Kraken Coding actively uses procedures to remove or to destroy any Personal Information once it is no longer needed to deliver our services or support. This is often in cooperation with third party cloud service providers.

- **Rights of Subjects:** To coordinate with our customers for any responses or inquiries regarding the processing of Personal Information as well as designing solutions permitting effective and efficient accessibility and portability of Personal Information within our products.

  Kraken Coding communicates with our customers to establish links with their data protection and security personnel to connect any data subject requests back to our customers in a timely and documented fashion.

- **Controls and Measures:** To put in place controls designed to protect privacy and safeguard Personal Information that Kraken Coding collects, uses, and discloses.

  Kraken Coding establishes controls for appropriate and necessary safeguards based upon industry best practices. Additionally, to ensure appropriate safeguards for customer environments we include an appropriate data management plan for each of our applications.

- **Data Transfer:** To provide appropriate assurances regarding data protection requirements related to any internal sharing or external disclosures outside the country of origin for the Personal Information.

Security Safeguards

Kraken Coding designs and uses controls relevant to ensure the confidentiality, integrity, and availability of Information Assets, especially including Personal Information, based on the STAR 1 and OWASP ASV standards, as applicable, to ensure that the specific privacy, security, and business objectives of Kraken Coding and our customers are met. Kraken Coding takes a holistic, coordinated view of the privacy and security risks in order to implement a comprehensive suite of controls and measures under the overall framework of a coherent management system.

- **Policies and Procedures:** To ensure consistent and comprehensive application of the appropriate and necessary controls and measures, Kraken Coding documents its privacy and security processes through policies, procedures, standards, work instructions, guidance, and other means.

  Kraken Coding maintains an Information Security Management System, based upon OWASP ASVS level 3 as part of its Integrated Management System that forms the framework for Kraken Coding risk management program. The Data Protection Officer is accountable for the functional attributes of the program though data protection, privacy, and security activities.

- **Organization:** To maintain appropriate accountability, Kraken Coding assigns personnel and third parties to roles that support data protection, privacy, and security responsibilities and to ensure the security of teleworking and use of mobile devices, Kraken Coding implements specific controls to protect InformationAssets.

  Kraken Coding manages risk through its Safety Management Plan overseen by the DataProtection Officer. Kraken Coding limits access by and use of mobile devices to Information Assets.

- **Human Resources:** To promote understanding by Kraken Coding employees and contractors that have access to Kraken Coding' informational assets, including customer data and Personal Information, throughout their lifecycle with Kraken Coding of their responsibilities as well as to ensure suitability for the roles for which Kraken Coding employees and contractors are considered.

  Kraken Coding requires that all personnel, both employees and contractors, agree in writing to confidentiality obligations regarding Information Assets, especially personal information, and acceptable use regarding TechnologyResources. Kraken Coding changes or terminates any access to Information Assets and use of Technology Resources of an employee or contractor when a role changes or upon leaving Kraken Coding.
  Kraken Coding require all staff to attend a mandatory annual cybersecurity training event.

- **Asset Management:** To ensure Kraken Coding identifies organizational assets and defines appropriate protection responsibilities as well as to ensure that information receives an appropriate level of protection in accordance with its importance to Kraken Coding and our customers.

  Kraken Coding classifies all categories of Information Assets that it maintains consistent with the relative risk rating to limit or restrict, as appropriate, any access or use.

- **Access Control:** To limit access as appropriate and necessary to information assets through the management of authorised user access with accountability of Kraken Coding employees and contractors to prevent unauthorized access to systems and services.
  Kraken Coding requires all end users have unique accounts with password complexity (not less than 10 characters in length, disallowing use of compromised values) consistent with NIST SP 800-63-3, Digital Identity Guidelines (specifically, NIST SP 800-63B, Authentication and Lifecycle Management, including Appendix A, Strength of Memorized Secrets). Remote access to Kraken Coding Information Assets is not permitted.

- **Cryptography:** To implement cryptographic controls protecting the confidentiality, authenticity, and/or integrity of information.

  Kraken Coding deploys at least AES-256 encryption for data-at-rest and at least TLS 1.2 (with SHA-256 and AES cipher suites) for data-in-transit to address the protection of Information Assets containing sensitive or personal information. This is in line with OWASP ASVS L3 guidelines.

- **Physical and Environmental:** To define secure areas for the prevention of unauthorised physical access, damage and interference to the organization's information and information processing facilities and to facilitate the protection of assets against loss, damage, theft or compromise of assets, and interruption to operations.

Kraken Coding maintains controls for its facilities (and ensure that its facilities partners, especially outsourced data centers) include specific physical access controls to prevent unauthorized access by establish a specific security perimeter and maintaining Technology Resources within a monitored facility with appropriate physical separation of environments.

- **Operations:** To operate systems and facilities in a secure manner protecting against malware, regular data backups are executed to protect against loss of data,logging and monitoring to record events and generate evidence. Managing operational software to confirm the integrity of operational systems, mitigating technical vulnerabilities as discovered, and reviewing information system audit rules to minimize the impact of audit activities on operational systems.

  Kraken Coding utilises secure third parties in order to perform backups of all environments containing Information Assets with planning and testing done consistent with ISO/IEC 22301, Security and resilience – Business continuity. Kraken Coding maintains virus and malware protection processes including enforcement of operation on all end user systems and at least weekly updates. Kraken Coding updates Technology Resources within appropriate timeframes as dictated by the risk rating associated with the vulnerability ensuring that critical updates as applied on an expedited basis to prevent operations without known protections. Kraken Coding periodically scans Technology Resources, including performing independent penetration tests and vulnerability scans on at least an annual basis, to monitor for any vulnerabilities or weaknesses.

- **Acquisition, Development, and Maintenance:** To implement security requirements as an integral part of information systems across the entire lifecycle, including those that provide services over public networks, and in our development and support processes to design those requirements as part of the lifecycle of our products and systems.

  Kraken Coding maintains Technology Resources using a formal configuration andtesting process that includes integration of available guidance for secure configurations. Kraken Coding implements processes that support a secure development process for its products and services.

- **Third Parties:** To address information security in our relationships with vendors, suppliers, and other third parties for the protection of Information Assets

  Kraken Coding only employs third party vendors for cloud solutions with relevant ISO and STAR accreditation capable of managing sensitive data.

- **Incident Response:** To respond to information security incidents consistently and effectively to address security events and weaknesses as well as mitigate risks to information assets, including customer information assets and Personal Information.
  Kraken Coding investigates discovered privacy and security events to determine if aprivacy and/or security incident has occurred and provide appropriate notification to customers and affected parties, including individuals, consistent with local law and regulation. Kraken Coding maintains an incident response 'Safety Management Plan' with specific procedures to address regional and customer requirements. All confirmed cybersecurity events are notified to AUSCERT cybersecurity.

- **Business Continuity:** To embed continuity of operations ensuring effective availability and integrity of information assets, which involves the planning and assessment of the business critical operations necessary for performance throughout and following an event impacting Kraken Coding and our customers.

  Kraken Coding follows a business continuity plan to ensure continued operations across its business functions and service delivery, including product and service support, during and following an interruption or disaster event.

- **Risk and Compliance:** To review ongoing compliance to avoid breaches of legal, statutory, regulatory or contractual obligations through information security assessments against Kraken Coding policies and procedures of implemented and operating controls and measures for information security.

Kraken Coding maintains external independent auditor reports for specific environments, especially those for the management of operational Information of customers. Kraken Coding performs company security gap analysis to ensure they are compliant with this policy and STAR / OWASP verification standards.

Training

- Data protection training is provided to each new Kraken Coding Personnel to ensure an understanding of privacy and information security fundamentals as well as internal policies and procedures for data protection processes (including this policy).
- All Kraken Coding Personnel receive data protection, privacy, and information security refresher training on an annual basis with specialized training provided for roles requiring additional knowledge concerning risks and vulnerabilities.
- Awareness and communications concerning risks and vulnerabilities are done on an ongoing basis and reviewed at the start of any project, internal or customer-related.

Security Incident Response

A security incident is any identified breach of access, data handling, or security policy. When identified, a security incident will be addressed with the highest level of response and will receive continuous effort 24/7 until any data risk is removed.

Kraken Coding has a clear Safety Management Plan established to ensure a consistent and effective approach to managing information security incidents, including communication on security events and weaknesses.

- All security incidents will be reported to Kraken Coding Data Protection Officer immediately upon detection. The Data Protection Officer will coordinate communication with the customer and affected parties.
- On confirmation all security events will be lodged with AUSCERT and the correct procedure followed as per AUSCERT guidelines.
- Separate procedures for the identification, collection, acquisition, and preservation of information that can serve as evidence in a disciplinary and legal actions is

maintained for each particular operational function affected or involved in an incident and the response.

- Disclosure of security incidents related to Managed Services customers will not be made public without specific written authorization from the customer
- Any incident that results in a data breach will follow Kraken Coding standard data breach procedure and notification processes in accordance with applicable law.
- For any security incident, the response will prioritize data protection. The relevant Kraken Coding response team will evaluate the risk and may prioritize data security over system availability.

Following any incident, Kraken Coding performs a post-incident analysis to identify the root cause of the incident as well as develop a set of lessons learned that can be used to determine if a Plan of Action & Milestone (POA&M) is warranted to follow up on the incident.

The incident response management includes the quantifying and monitoring the types, volumes, and costs of information security incidents and the information gained from the evaluation of information security incidents is used to identify recurring or high impact incidents. With due care of confidentiality aspects, Kraken Coding uses anecdotes from actual information security incidents in user awareness training as examples of what could happen, how to respond to such incidents, and how to avoid them in the future.

Data Protection

Kraken Coding privacy and security controls are consistent with the obligations under the Australian Privacy Act (1988).

Kraken Coding undertook several actions, some of which are ongoing:

1. We have appointed a **Data Protection Officer**, as noted above.
2. We have processes in place to perform Data Protection Impact Assessments (DPIAs) as a part of our Safety Management Plan, when necessary to understand what if any risks exist to the rights of

individuals are impacted by data processing and to identify appropriate and necessary mitigations to address the recognized risks.

3. We have ongoing organizational activities such as training and awareness on data protection for employees.

4. We have put in place requirements to document decisions related to data protection so that our actions and processing can be explained and properly understood.