Supplier Information Security Guidelines and Requirements

Greetings!

The institute is in the process of seeking to be certified on Information Security Management System, ISO 27001:2013. In compliance with the requirements of this standard, we would like to bring your attention to the following requirements on our engagement (see attached file). Feel free to give us your feedback and input. You can also visit our website (karumotti.ac.ke) on the **resources** section, **Downloads** to familiarize yourself with the institute's **information security policy** and other relevant supporting policies.

By entering into any contract with Karumo TTI as a supplier/service provider, you shall:

1. Treat all information provided by Karumo TTI as confidential and shall not disclose, reproduce, or use it for any purpose other than fulfilling the obligations outlined in this agreement. Confidential information includes, but is not limited to, business plans, customer data, and applications or systems that exclusively belong to Karumo TTI.
2. Comply with all applicable data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR). Compliance with relevant information security standards and regulations, such as ISO/IEC 27001, and any industry-specific standards applicable to the services or products provided is included also. Implement appropriate technical and organizational measures to ensure the security and confidentiality of personal data processed on behalf of Karumo TTI.

NB: In addition to the above, any supplier of information communication technology services, systems or products shall (as applicable):

1. Implement strong access controls and authentication mechanisms to ensure that only authorized personnel can access, modify, or interact with Karumo TTI's information.
2. Implement and maintain encryption measures to protect sensitive information.
3. Promptly report any security incidents or breaches to the institute. Similarly, any security breach or incidence that may be detected by the institute shall be promptly reported to the service provider for appropriate remedial action.
4. Put in place robust business continuity and disaster recovery plans to ensure the availability and integrity of the institute's information in the event of disruptions.
5. Have a robust change management process to assess and approve changes to IT infrastructure components, ensuring that changes do not introduce security vulnerabilities.
6. Ensure that any subcontractors engaged adhere to the same information security requirements and standards as outlined above.

Approved by: Flora Kanyua__________ __________Date: 09/02/2024_______

Principal Karumo TTI

Issued by: Dennis Bangi_________ _______________Date___09/02/2024______

Management Rep. Karumo TTI