POLICY 9: COMMUNICATION, DATA AND INFORMATION SECURITY

This policy aims to establish guidelines and procedures for safeguarding GNE's communication, data, and Information stored on computer equipment, systems, and software against accidental or deliberate threats and risks from within GNE and outside. This comprehensive policy aims to protect all Information pertaining to GNE, including its products, customers, suppliers, business partners, and shareholders. By ensuring confidentiality, integrity, and availability, the policy contributes to business continuity and minimizes the risks of business damage due to security threat incidents, aligning with international standards.

Data Protection And Privacy

At GNE, we take the protection of personal data seriously. Our commitment is to safeguard the Information of our customers, employees, and third parties by strictly following the law. Data and Information are handled ethically, using them only for legitimate reasons and keeping them for the necessary time. We follow agreements and adhere to laws during any transfers regarding third-party data. Our Legal Department reviews and signs non-disclosure agreements as needed to ensure extra confidentiality. This reflects our dedication to maintaining high standards in handling and protecting data**.**

A. GUIDELINES

This policy applies to all employees, contractors, and third-party entities with access to the organization's communication channels, data, and Information. Employees are mandated to understand and adhere to organizational policies. Business-related communication must exclusively occur through approved channels, utilizing encryption for sensitive Information. Strict adherence to data classification and access controls is crucial to ensure the secure handling and protection of GNE's data and Information. Personal use of social media applications should be discreet and in compliance with applicable laws, rules, and regulations, as well as Gerab's policies, standards, and guidelines, including Gerab's office and Information and Technology guidelines, as well as organizational values.

The Information Communication Technology Department (ICT Dept.) will design procedures, standards, and guidelines to ensure compliance with data security controls. The Internal Audit Department will evaluate security control procedures and ensure adequate compliance with this policy.

B. EMPLOYEE RESPONSIBILITIES:

I. Dealing with External Parties

Definition: External parties may include Clients, Suppliers, Partners, Media, Government Agencies, Regulatory Authorities, Financial Institutions, Competitors, Consultants or Contractors, Industry Associations, and Community Organizations.

i. At the time when our Clients, Suppliers, and Partners request Information relating to Gerab's compliance with stipulations relating to Sanctions, Embargoes, and Anti-Money Laundering, employees must follow these guidelines :
   - Refrain from responding directly to the parties seeking this Information, acknowledge the receipt of the request, and inform with a commitment to responding to them at the earliest;
   - Obtain opinion and response from the Legal and Compliance function and respond accordingly to the requesting party.

ii. During Trade Shows/Exhibitions /Media interviews, employees should avoid providing inaccurate, incomplete, or material Information to visitors and representatives from the media.

iii. All external inquiries that are sensitive in nature and seek Information regarding GNE or its employees, directors, products, services or operations, etc., must be referred to the Department Head, who, in coordination with SVP Corporate Excellence & HR and the Legal and Compliance function, will provide the most appropriate response to these queries.

II. Dealing with Intellectual Property

Definition: At Gerab, the purview of Intellectual Property extends to include trademarks, research, products, customer and supplier information, technical standards, processes, IT systems, and articles developed by employees during their tenure with GNE. The confidential nature of these assets necessitates effective data management to preserve and protect them from being copied and cloned by external entities to cause harm or to gain a competitive advantage.

i. Employees must understand and be aware of Gerab's definition of Intellectual Property and its value as corporate assets, requiring proper usage and management to preserve their validity and worth.

ii. Acknowledge the critical role of Intellectual Property in sustaining Gerab's competitive advantage and how its misuse can result in detrimental consequences, thus emphasizing the importance of responsible handling.

iii. Employees, including those affiliated with Gerab's subsidiaries and associates, are responsible for actively working to prevent Intellectual Property infringements to safeguard Gerab's interests.

iv. Be aware that Gerab's Marketing and Legal Department are responsible for acquiring the registration of trademarks, ensuring legal protection for these valuable assets.

i. Recognize the critical role of Intellectual Property in maintaining Gerab's competitive advantage, with the understanding that misuse can lead to severe consequences.

III. Dealing with Electronic Data and Communication

Definition: Electronic Data and Communication involve responsibly using digital channels while following specific protocols to guarantee the secure and confidential transmission of information. This includes adhering to IT guidelines, using secure communication channels for official correspondence, avoiding sharing sensitive data through unsecured means, employing encryption for confidential information in emails, and implementing file passwords.

i. Adhere to standards, procedures, and guidelines specified by the Information Technology Department from time to time.
ii. All employees should ensure that all official communication is conducted through the GNE's secure electronic communication channels, specifically for emails, to protect against potential system breaches and hacks.
iii. Sensitive Information must not be shared through unsecured email channels.
iv. Encryption protocols must be employed for emails containing confidential data.
v. Implement passwords for files that are being transmitted.

IV. Dealing with Personal Data

Definition: At GNE, protecting personal data is considered crucial to ensure privacy and compliance with local and international data protection regulations. Personal data refers to information about a person that can directly or indirectly identify them. This encompasses names, contact details, identification numbers, online presence, and any other data reasonably linked to a specific person. At GNE, safeguarding personal data is crucial to ensuring privacy and compliance with local and international data protection regulations.

i. Employees are required to identify and classify personal data within their possession clearly. This understanding aids in recognizing the sensitivity and importance of such data.
ii. Employees must obtain consent from individuals during the collection and processing of any personal data. Clear communication regarding the purpose of collecting personal data is essential to ensure transparency.
iii. Only data that is necessary by law or required to adhere to local procedures will be collected. This practice ensures that data collection is purposeful and in compliance with relevant regulations.
iv. The guidelines outlined in the 'Dealing with Confidential Data' section, the next segment, must be followed rigorously when handling any personal data. This ensures a consistent and secure approach in managing sensitive information.

V. Dealing with Confidential Data

Definition: Confidential data, as defined by this policy, encompasses sensitive information not intended for public sharing. This includes personal details, financial records, business

processes, trade secrets, and other classified information. Access to this data is restricted to authorized individuals only, and any unauthorized use or disclosure may result in disciplinary or legal action. The protection of confidential data is of paramount importance to comply with regulations, uphold privacy standards, and prevent potential data breaches.

i. Maintain full confidentiality of everything in their knowledge resulting from performing the employment, whether relating to the business of GNE or concerning the business of any person or business entity having dealings with GNE.
ii. Avoid retaining for personal use; copy, licensed application software, technical manuals, reports, commercial proposals, and any other technical, commercial, or administrative material and computer-stored data to any third party unless required to do so by or with the concurrence of the management of GNE.
iii. Refrain from publicly discussing any Company-related matters or those relating to clients, business partners, suppliers, employees, etc.
iv. All confidential documents should be stored in locked file cabinets or rooms accessible only to those authorized to access the data or Information.
v. All electronic data should be password protected, following the encryption protocol, and must be updated regularly.
vi. Employees should clear their desks of confidential Information and store them securely before leaving the office at the end of office hours.
vii. Employees should refrain from leaving confidential Information visible on their computer monitors when they leave their workstations.
viii. All confidential information in written documents or electronically should be marked as "Confidential."
ix. Obsolete data and Information should be disposed of by following the Disposal guidelines (e.g., Avoid printing confidential documents and disposing them away without being shredded)
x. Refrain from using Gerab's name, logo, trademarks, or facilities for commercial purposes unrelated to their job, including outside work (including on letterhead or websites).
xi. Employees should report any observed or suspected security incidents to their manager or department head.
xii. Upon termination, the employees shall immediately hand over to their authorized representative all statistics, documents, records, memoranda, papers, and electronic storage devices that relate in any way to the property, business, or affairs of GNE and its subsidiaries.

VI. Dealing with Media (Including Social Media) Enquiries

Definition: Media inquiries (including social media) refer to requests for information, comments, or interviews from representatives of traditional media outlets (such as newspapers, television, and radio) and inquiries from individuals or entities through social media platforms. This may include questions or requests for official statements, interviews, or any form of engagement seeking information related to GNE's activities, events, or other matters of public interest. Managing media inquiries involves providing accurate and timely responses, coordinating communication strategies, and ensuring alignment with the GNE's messaging and values.

i. All Media, including social media, inquiries should be channeled through GNE's Marketing Department, which will coordinate responses following company rules and policies.
ii. The Marketing Department is responsible for ensuring accurate public information about our operations when necessary.
iii. Employees should never act as unauthorized spokespersons for GNE; only authorized spokespersons can make public statements (including on social media platforms).
iv. Non-compliance with these guidelines may result in disciplinary action.

VII. Dealing with Social Media

Definition: Social media, here, refers to online platforms and communication channels that enable users to create, share, and interact with content. This includes but is not limited to websites and applications where individuals can post text, images, and videos and engage in virtual communities.

i. Employees are prohibited from using social media applications for personal browsing, chats, and posts during official working hours. This restriction aims to prevent interference with daily work activities and deliverables, ensuring optimal productivity for GNE.
ii. GNE's computer systems, official phones, or any other provided gadgets must be used exclusively for business purposes. While social media platforms can be used for work-related activities, employees should exercise prudence, especially when using apps like WhatsApp and LinkedIn for official messages.
iii. Employees must never discuss or disclose confidential financial or other non-public, proprietary company information while using social media for personal or permitted business reasons.
iv. Avoid sharing confidential information regarding GNE clients, shareholders, vendors, suppliers, or business partners.
v. Employees must refrain from posting opinionated or derogatory remarks on Religion, Political Leaders, Monarchs, and/or Government on social media sites.

vi. Non-compliance and failure to adhere to these guidelines may result in disciplinary action.

C. ADDITIONAL RESPONSIBILITIES OF MANAGERS/DEPARTMENT HEADS

i. Ensure that their teams comply with all applicable laws and regulations related to communication, data, and information security.
ii. Responsible for implementing and maintaining information security policies that outline the proper handling, storage, and protection of sensitive data and information.
iii. Responsible for managing the data classification system to identify and protect sensitive data and information.
iv. Manage access controls to ensure that only authorized personnel have access to sensitive data and information.
v. To protect them from unauthorized access, managers should ensure that sensitive data and information are encrypted in transit and at rest.
vi. Manage the vetting and monitoring of third-party vendors to ensure they meet GNE's data and information security standards.