Intellectual Property Policy and IT implementation

1.Overview

Nera Kritis SA acknowledges that the intellectual property of customers is of utmost importance as well as the need to safeguard it. All stakeholders should feel safe that the intellectual property entrusted to Nera Kritis SA is treated with confidentiality and measures are taken to protect all customers intellectual property (IP from now on).

2.Purpose

The purpose of this policy is to define the guidelines, rules and regulations for the proper usage, security and maintenance of the company's digital assets. In addition, guidelines are provided to ensure the safety, integrity and security of the products, data, services for the services offered to Nera Kritis SA's customers.

3.Scope

This policy applies to all employees, contractors, subcontractors and all other persons or corporations tied to Nera Kritis SA by an NDA agreement. This policy also applies to all digital equipment (PCs, Laptops, Tablets, Smartphones) issued by Nera Kritis SA to its employees and partners. This policy also applies to personal digital devices as long as company software or company data is stored in them. Technical implementations that could allow remote access to Nera Kritis SA's systems or networks are also included.

4.Policy

It is the responsibility of Nera Kritis SA, employees, contractors, subcontractors, guests and others with access privileges to Nera Kritis SA's networks and systems to ensure that their access connections, whether on a working site or remote, meet all necessary security requirements and conform to all Nera Kritis SA's policies. Access to the Nera Kritis SA network is strictly limited to authorized users as instructed and maintained by the IT dpt. Access privileges to Nera Kritis SA's networks and systems may be declined, suspended, or revoked at any time for violations to policies or operating procedures. Authorized users accessing Nera Kritis SA's networks and systems from a personal or other non-business issued computing device are responsible for preventing access to any Nera Kritis SA computer resources or data by non-authorized users. Performance of illegal activities through the Nera Kritis SA network by any user authorized or otherwise, is prohibited. All authorized users bear responsibility for the consequences of misuse of network and system access privileges.

For additional information regarding Nera Kritis SA's remote access connection options, including how to obtain a remote access login, troubleshooting, etc., contact the IT dpt at it@Nera Kritissa.gr .

4.1 Network and system access

4.1.1 Access to Nera Kritis SA's network is usually made available after the hiring process and the induction period has concluded and a request is made by the head of corresponding dpt to the IT dpt. Prior to the activation of relevant accounts that provide access to Nera Kritis SA's systems, an NDA document needs to have been signed. Specific department such as Engineering, Sales, Sourcing, Finance and CIS are subject to additional layered access privileges that can change and are based on job requirements. This may involve increasing level of granted rights for specific amounts of time depending on current assignments, which is decided by both CIS (Continuous Improvement Strategy) and IT dpts.

4.1.2 Technology account credentials must conform to the security requirements articulated by IT dpt.

4.1.3 All system accounts will be issued and managed by IT dpt in accordance with its procedures for identity and access management.

4.2 Prohibited Uses and Actions

4.2.1 Use for purposes that violate Greek legislation, including copyright laws that prohibit the downloading or distribution of copyright protected data such as. Drawings, music, video, videogames, etc.

4.2.2 Use for a private enterprise or not-for-profit organization unless authorized by Nera Kritis SA.

4.2.3 Use in any way that interferes with or disrupts other network users, services, or equipment.

4.2.4 Accessing sites that are pornographic or offensive in nature.

4.2.5 Accessing or attempting to access restricted data files, software or systems without authorization.

4.2.6 Creating or transmitting lewd, obscene, hateful, bigoted, or discriminatory material or information in line with Nera Kritis SA's anti-harassment policy.

4.2.7 Concealing or misrepresenting one's name or affiliation to mask irresponsible or offensive electronic communication.

4.2.8 Using electronic mail or other network communications to harass, offend, or annoy other users in line with Nera Kritis SA's anti-harassment policy.

4.2.9 Sending chain letters through electronic mail.

4.3 Remote access

Nera Kritis SA through its IT dpt provides secure VPN access to on-site resources from offsite. This VPN service also allows authorized users to create a secure connection between their remote computer and the private business network, allowing access to systems and devices including assigned PC's, laptops, and network storage devices. Policies and procedures for obtaining and using VPN access are as follows:

4.3.1 Use of external resources to conduct Nera Kritis SA's business must be approved in advance by the IT dpt.

4.3.2 Employees must make requests for remote access to their supervisors, who must initiate requests to It dpt on their behalf.

4.3.3 Everyone accessing the VPN must authenticate, using his account credentials. VPN accounts are disabled when users' are disabled upon termination of employment.

4.3.4 Users are removed when directors or department chairs make a request for removal, or when technology staff are made aware of employment terminations.

4.3.5 Authorized users shall protect their login and password, even from family members.

4.3.6 While using a Nera Kritis SA-owned computer to remotely connect to Nera Kritis SA's network, authorized users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control.

4.3.7 All hosts that are connected to Nera Kritis SA's internal networks via remote access technologies must use the most up-to-date anti-virus software; this includes personal computers.

5. Policy Compliance

5.1 Compliance Measurement

The IT dpt will verify and promote compliance to this policy through various methods, including reports, internal audits and feedback to individuals or departments.

5.2 Exceptions

The head of IT dpt must approve any exception to the policy in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to network access revocation and personal disciplinary action, up to and including termination of employment.