Prepared: Support Function
Approved: Daniel Tedesco
Security Class: Internal

Document no: DEK-21:0061
Revision: A
Date: 30/6/2021
Document Type: Policy

DEK Technologies Vietnam ICT Policy

1 Purpose

This document contains additional clauses that apply specifically to staff of DEK Technologies Vietnam, above and beyond those described in the "DEK Technologies Employee ICT Policy and Procedure" [1].

2 Effective Date

This version of the policy is effective from the 1st of July 2021.

3 Principles

Members must always be security conscious and think carefully about security before taking any action.

In our industry the importance of data security and privacy is paramount. Our customer’s primary concern is about protecting their product and information. They rely and trust us to follow the best practices to protect their business.

Every member must follow every rule without exception, otherwise it will:

- Break the customer’s trust
- Badly impact the customer’s business
- Badly impact the relationship between DEK and its other customers
- Badly impact the ability for DEK to win future new businesses
- Badly impact your career and your fellow member’s career, in the IT industry

The importance of security in the modern world cannot be overstated. The weakest link when it comes to security is people and their actions. Do not be the weak link.

4 Policy

4.1 Network

By default, DEK Technologies Vietnam Work From Home (WFH) users must have GlobalProtect VPN connection established on their laptops at all times. Working activities such as applications installed, browser history logs, etc., will be logged daily (during WFH period) by the ICT team and stored for audit purposes. For some specific projects approved by the customer, separate customer provided VPN solutions shall be used instead of DEK Technologies Vietnam GlobalProtect VPN solution.

4.1.1 Customer Engineering Network

Customer engineering networks, which have site-to-site and client-to-site Virtual Private Network (VPN) connections to customer sites, must only be established on DEK Technologies Vietnam devices. No personal or other devices are permitted to establish and access customer engineering private networks.

Token application for two factors authentication solutions must be setup on smart phones only. No desktop or laptop token applications are allowed.

4.1.2 Internal Engineering Network

Internal engineering networks, which have internal and internet access provided via Ethernet cables, are using MAC address filtering security to limit the access to approved devices only.

Internal engineering networks, which have internal and internet access provided via WiFi, are using the 802.1x standard. This standard combines certificates and domain user accounts provided by the DEK Technologies Vietnam domain controller, and is deployed to approved devices only.

4.1.3 Internship Network

Internship networks, which have internship projects access and internet access provided via Ethernet cables, are using MAC address filtering security to limit the access to approved devices only.

Internship networks, which have internship projects access and internet access provided via WiFi, are using a Dynamic Keys solution. This solution generates WiFi access keys based on MAC addresses of the approved devices.

4.1.4 Human Resource and Finance Network

Human Resource (HR) and Finance networks, which have internal and internet access provided via Ethernet cables, are using MAC address filtering security to limit the access to approved devices only.

Human Resource (HR) and Finance networks, which have internal and internet access provided via WiFi, are using the 802.1x standard. This standard combines certificates and domain user accounts provided by the DEK Technologies Vietnam domain controller, and is deployed to approved devices only.

Only General Manager network and ICT Admin network can have access to Human Resource (HR) and Finances networks.

4.1.5 Guest network

Guest networks have WiFi time-limited internet access only.

4.2 Personal Computer Equipment

Users are not allowed to bring personal computers to the DEK Technologies Vietnam office without prior written and signed approval from the ‘Authority’ (See section 5).

DO NOT bring your personal laptop to the office without permission
DO NOT bring laptop home
DO NOT use USB stick
dek

4.3 Physical Security

4.3.1 Building Access

Building access is controlled by an Access Door Control (ADC) system for door access at the main door, basements and lifts. Users need to use card and security code to access the office.

For some specific customers, access to working areas shall be restricted to only engineers of those projects.

The building access is also always controlled by a security guard; 24 hours, 7 days a week, 365 days a year. Camera monitoring system is in place to provide evidence for unauthorized access to the office.

Visitors to the building are required to sign-in.

There is a Fire alarm system and rescue team for critical situations.

4.3.2 Client Machines

Individuals are responsible for security of the client machines allocated to them, particularly with respect to laptops taken outside the secure office environment.

MAC address filtering and domain certificate-based authentication methods are deployed to ensure network access is provided to authorized client machines only. This is done down to the working position level.

Customer provided laptops need to be registered with ICT before using at DEK Technologies Vietnam.

Laptops may not be removed from the DEK Technologies Vietnam office unless written permission is provided by the ‘Authority’ (See section 5)

4.4 Use Of Computer Facilities

4.4.1 General

Users shall follow the approved “software permitted list” which defines software eligible to use at DEK Technologies Vietnam office.

Users shall not connect any USB hard disk, USB stick and other external storage to any machine. (User machines are configured to prevent access to external drives via USB.)

4.4.2 Data Theft Prevention

Internal Cloud-based services are used for team work.

Separate Cloud-based public services in De-Militarized Zone (DMZ) at DEK Technologies Vietnam office are used to share data with customers (following customer requirements).

INFORMATION
(Code, documents, emails, salary, etc.)
is CONFIDENTIAL:
DO NOT
SEND INFORMATION TO
PRIVATE EMAILS (E.G. PERSONAL GMAIL)
DO NOT
SEND INFORMATION
TO PEOPLE OUTSIDE OF DEK
AND YOUR PROJECT'S RELATED
KEEP IT SECRET
DO NOT
ATTACH CUSTOMER /
PROJECT'S DOCUMENTS
TO THE EMAILS
dek TECHNOLOGIES

4.4.3 Access Limitations

By default, there is a permanent limited access to GitHub, GitLab, etc., (in particular a block on uploads). DEK Technologies Vietnam follows the customers rule to permit the use of GitHub or external resources, when approved by the customer for specific projects.

Separate application permitted lists are deployed for specific engineering networks, to limit access to working resources for business purposes only.

Social media access is limited to non-working time.

dek TECHNOLOGIES
CUSTOMERS' INFORMATION IS OWNED BY THE CUSTOMERS AND DEK HAS THE OBLIGATION TO PROTECT IT.
DO NOT PUT CONFIDENTIAL INFORMATION (DOCUMENTS, SOURCE CODE...) ON PUBLIC REPOS E.G GITHUB, GITLAB...
DO NOT UPLOAD INFORMATION TO PUBLIC CLOUD.
DO NOT PUT CONFIDENTIAL INFORMATION ON PUBLIC CHAT (SKYPE, VIBER, ...)

5 Authority

For the purpose of preceding text, the Authority is defined as persons belonging to the management and/or ICT or IS groups. For more detailed specification of Authority, see site specific documents.

6 Responsibilities

ALL DEK Technologies Vietnam members are responsible to strictly follow this policy. If any member becomes aware of any violation of this policy, they should immediately escalate to the Authority.

7 Reference documents

[1] DEK Technologies Employee ICT Policy and Procedure