OPENLM

OpenLM Device Management and Teleworking Policy

Version:	**2**
Approval date:	**01.09.2022**
Developed by:	**Vasile Tarlev - IT Security**
Approved by:	**Branislav Potocek - VP Operations**
Responsible to enforce:	**Vasile Tarlev - IT Security**
Classification:	**Information security policy / Internal unrestricted use**
Pages:	**4**

Policy Revision

Version	Date of revision	Description of changes / review	Approved by
2	17.07.2023	Policy review & update	Branislav Potocek

I. Introduction

1. The use of personal devices while remote working is encouraged in order to offer employees the commodity and the possibility to fulfill their work assignments remotely.
2. At the same time, privately owned devices pose a significant risk to data security if mismanaged and if the appropriate security procedures are not followed. These devices may be a link of unauthorized access to the organization's data and IT infrastructure.

II. Objectives and scope

3. The purpose of the policy is to define a set of rules concerning device security management, and to establish a good practice regarding managing both company's owned and privately owned devices, in order to reduce the security risks and to offer employees the option to work remotely.
4. The scope of the policy extends, but it is not limited, to all digital devices (mobile or not), owned by the company or by employees, including smartphones, tablets, personal laptops, or any device capable of computing and storing company data or has access to the company's networks or systems and are used in this sense.

III. Principles

5. Using privately owned digital devices is optional and employees are free to choose the appropriate means and tools by which they fulfill their work assignments.
6. Regardless of what devices are being used, employees must ensure the minimum set of security requirements and comply with company's security policies.
7. Use of privately owned devices for work related assignments is prohibited if the security requirements are not met and the employee does not enforce the security policies, thus exposing the company to threats.
8. Exceptions from this policy may result from urgent and extreme cases only, when setting the security requirements may be time consuming and goes against the nature of an extreme or urgent situation. Such cases must be notified to the IT Department.
9. In case of any suspicious activity, loss of access or loss of data, employees must notify the IT Department.

IV. Physical security requirements

10. It is strongly discouraged to use any devices (privately-owned or not) for any work-related tasks using a public internet connection.
11. Employees must immediately report any lost or stolen devices that had access to the company's system or contained any of the company's information (privately-owned or not).
12. Employees must ensure the physical security of their devices and ensure that unauthorized people do not have access to their devices. Physical access dismantles any digital controls & restrictions, therefore a device is much more exposed to attacks where physical access is unrestricted to unauthorized people.

V. Remote access and authentication

13. It is prohibited to use any public networks for work. In case of necessity, access to

company’s resources and system in public areas must be done on mobile private networks (hotspot) and only while using the company approved VPN.

14. Employees must have two factor authentication enabled on every application & service that offers it.
15. While working remotely, on company or privately owned devices, employees must follow the principles of secure configuration and implement a set of minimal requirements while setting up their working environment:
    a. change the default passwords for the personal router or any other home network devices;
    b. change overly permissive default configurations on applications installed;
    c. if possible, make use of the security features offered by the software / hardware installed;
    d. create another separate user on their personal computers, from which they will access the company's systems and data. In case this is not possible, it is advised to use a separate browser, dedicated for work related activity only. By segregating such channels, security risks are diminished.
16. OpenLM may introduce a solution to secure and control endpoint devices. The goal is to enforce security configurations, auto patching, password requirements,screen-lock, remote wipe capabilities and deployment of additional policies.
17. Remote workers shall connect to OpenLM resources & infrastructure only by VPN. The solution provided by the company is OpenVPN.

VI. Endpoint security

18. Software must be installed only from official and trusted vendors. It is prohibited to install cracked or pirated software as it is both illegal and extremely dangerous for the entire infrastructure of the company.
19. Employees shall uninstall old or unnecessary applications. Otherwise these applications need to be patched or updated.
20. Antivirus shall be enabled and kept updated. The company endorses the default OS provided anti-virus (windows defender). Linux users will use ClamAV.

VII. Data protection and confidentiality

21. Employees shall use means of encryption & cryptographic solutions while transferring data, connecting to the network, etc.
22. Employees shall use only company approved channels of communication - Gmail, Google Chat, Microsoft Teams, Zoom, Zoho.
23. Company files & documents shall be sent only through approved channels of communication - Gmail, Google Chat.

VIII. Breach of policy

24. For violating any of the company’s policies and for exposing the company to security risks, an employee may be subject to disciplinary actions or penalties and review of access rights to company’s information.

25. Each violation will be assessed individually, and measures will be taken proportionately to the gravity of the offense committed.

IX. Other provisions

26. Every exception from this policy should be individually inspected and documented with a reasonable explanation for why the exception is needed.
27. The policy and its requirements shall be applied in a non-discriminatory manner by all employees of the company.
28. The policy will be revised and updated if needed every year or every time a change is required considering the security needs or infrastructure changes of the company.
29. The policy takes effect on the date of its approval.

X. Policy exceptions

Describe the exception	Exception approved by
-	-