Subject: **MPS Monitor - eXplorer 3.9 Software Safety and Compliance Certification**

We hereby certify that the MPS Monitor eXplorer 3.9 software, manufactured by our company, does not contain any viruses, malware, nor threats of any kind to the information security of the Customers.

The eXplorer 3 software has been developed in compliance with the OWASP Top 10 international specifications and guidelines and is subject to continuous testing and verification by independent institutions that certify compliance with these guidelines.
The code of the eXplorer 3 software, before the release of each version, is subject to Code Review and static analysis by specialized cybersecurity firms, to verify that:

- the installation package contains only software modules digitally signed by MPS Monitor srl to guarantee its authenticity
- the software does not contain known vulnerabilities of high criticality, and that any vulnerability previously found has been eliminated before the release of each new version
- The software is not detected as malware by the most popular antivirus products on the market.

All access methods, API interfaces and web endpoints used for communication between eXplorer 3 and the MPS Monitor cloud systems are subjected to Penetration Tests on a regular basis, usually every quarter, in order to verify the system's safety and compliance with international standards and guidelines. The process of automatic update of the software is subject to a specific Penetration Test process every year to verify the security against possible attacks in the update supply chain.

The information collected through the software is processed within an Information Security Management System that is certified in compliance with UNI CEI ISO/IEC 27001:2017; certificate no. 50 100 13777 Rev. 003 was issued by TÜV Italia srl on 06/03/2020 and is available at the following link: http://www.mpsmonitor.it/docs/iso-27001.pdf.
MPS Monitor srl adopts information security policies compliant with AICPA SOC 2, and undergoes an annual audit by A-LIGN to certify compliance with the defined Trust Services Criteria (**Security, Availability, Confidentiality).** The SOC 2 Audit Report issued by A-LIGN is available for download in the MPS Monitor Portal after e-signature of a specific Non Disclosure Agreement (NDA).

MPS Monitor srl adopts company policies aimed at adhering to regulatory requirements on privacy and information security, and processes data in full compliance with the provisions of Regulation (EU) 2016/679 of the **European Parliament and of the Council** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). With particular reference to the GDPR, the MPS Monitor software is produced and operated in compliance with the principles laid out in said European regulation and, in particular, with the principles of "*data protection by default and by design*". The protection of personal data is pursued as early as the design stage.
eXplorer 3 is developed to collect and process data relating to printing devices connected to the Customer's network, in order to manage them in a correct and effective way. The operations carried out are directly connected to this specific purpose. In particular, the software does not collect any data relating to the type or content of documents printed, to users who print them, nor to natural or legal persons whose data is processed through said devices and/or documents.
The data is collected from the printers using the eXplorer 3.x software module, which has the following technical specifications and features:

1. It is installed on a hardware device (PC or printer) within the Customer's network and with Internet access (port 443 / HTTPS). The device should connect to the printers on the network using the SNMP protocol (port 161 / UDP).
2. In order to exchange data and receive information about tasks to be performed, the software connects (usually sending a ping once every 5 minutes) to a Server that can be reached through different domain URLs https://*.abassetmanagement.com or https://*.mpsmonitor.com.
3. At set and configurable times (generally three or more times a day) and based on the information made available by the Server, eXplorer 3 performs a UDP scan of the subnetworks or IP addresses where the printers can be installed; the times and subnets or IP addresses to be scanned are defined in a special administration function on the configuration pages of the MPS Monitor Portal.
4. It identifies all printer-type devices, while completely omitting all other network devices of any other nature.
5. Data collection generally takes a few seconds or minutes, depending on the complexity of the network and number of devices.
6. By using UDP, the traffic is minimum and it does not have any noticeable impact on the network and devices.
7. The data collected by the printers are stored in CSV and XML format in the \Agent\send folder of eXplorer 3 installation path, so that the customer can have access to the files and check what information is collected every time the scan is performed.
8. In case problems are found when reading data from a printer model, the system uses the

SNMPWalk command to generate additional files with information on the entire MIB of the printer; these files have .WLK extension and allow us to identify and solve problems when reading data. This function can be disabled when configuring the eXplorer from the MPS Monitor Portal.

9. CSV and WLK files are transferred via HTTPS to MPS Monitor servers on cloud. All communications between the eXplorer 3 software and the MPS Monitor Portal take place exclusively using the HTTPS protocol.

10. The data in the files is used to update the Database that manages the Client's printers.

Under no circumstances will the Customer's network be accessible from the outside. Therefore, the installation of the eXplorer 3 within the Client's network does not pose any security risk to the network itself.

Milan, 23 March 2022
MPS Monitor srl
Chief Executive Officer
Nicola De Blasi