Virtual Machine Usage Policy for Training Participants

Effective as of: 20 June 2025

1. Purpose and Scope

This policy (hereinafter: “Policy”) sets out the rules for using virtual machines (hereinafter: “VM” or “Virtual Machines”) provided to participants (hereinafter: “Participant” or “User”) during training organised by **Sages sp. z o.o.** (hereinafter: “Organiser”). The aim of the Policy is to ensure safe, lawful and ethical use of the infrastructure and to limit the Organiser’s potential legal liability.

2. Definitions

1. **Virtual Machine (VM)** – a dedicated, isolated computing environment made available to the Participant by the Organiser solely for the duration and purposes of the training.
2. **System** – the entirety of technical infrastructure and software within which the Virtual Machines operate.
3. **Training Materials** – content and resources provided to Participants by the Organiser as part of the training.
4. **Prohibited Activities** – any actions that are illegal, contrary to this Policy, contrary to good practice or that infringe third-party rights.

3. Access Conditions

1. The Organiser grants the Participant access to the VM for the duration of the training under the terms set out in this Policy.
2. Access credentials are personal and must not be shared with third parties.
3. Login details are confidential; the Participant must keep them secret at all times.

4. Rules of Use

4.1 Permitted Activities

1. Performing tasks specified in the training programme.
2. Installing and configuring software necessary to complete the exercises, provided that this does not violate section 4.2.

4.2 Prohibited Activities

1. Using the VM for any unlawful activity, in particular: a. unauthorised access to IT systems (hacking, phishing, etc.); b. distribution of malware; c. infringement of copyright or licence terms (piracy, unauthorised sharing of content, cracks, “warez”); d. storage, processing or sharing of illegal content (e.g. child sexual abuse material, hate speech, extremist content); e. conducting DDoS attacks, port scanning or any activity that interferes with third-party systems.
2. Modifying the System’s security settings without the Organiser’s consent.
3. Sharing VM resources with other persons.
4. Using the VM for commercial or private purposes not related to the training.

5. Monitoring and Logging

1. All activity within the System may be monitored, logged and analysed by the Organiser or entities authorised by the Organiser.
2. Logs may be used for security, system development and, where necessary, to demonstrate compliance with the law.
3. By starting to use the VM, the Participant consents to such monitoring and logging.

6. Personal Data Protection and Confidentiality

1. The Organiser processes Participants’ personal data in accordance with applicable legislation (in particular the GDPR) only to the extent necessary for the training.
2. The Participant undertakes not to process in the VM any personal data that are not required for the exercises.
3. The User is responsible for the confidentiality of any data that they introduce into the VM.

7. Participant Liability

1. The Participant bears full civil, criminal and administrative liability for their actions within the VM.
2. The Participant undertakes to indemnify and hold the Organiser harmless from any claims by third parties arising from the Participant’s Prohibited Activities.

8. Organiser’s Liability

1. The Organiser exercises due care in maintaining the System but is not liable for damage resulting from improper or non-compliant use of the VM by the Participant.
2. The Organiser is not liable for content generated or stored by Participants in the VM.

9. Breaches and Sanctions

1. If a breach of the Policy is detected, the Organiser may, at its discretion: a. block or restrict access to the VM; b. exclude the Participant from the training without refund; c. inform the relevant law-enforcement authorities or take legal action.
2. Measures taken under section 9.1 do not preclude the Organiser’s right to seek damages.

10. Security Incident Reporting

The Participant must promptly inform the Organiser of any security incident, irregularity or suspected breach of this Policy.

11. Final Provisions

1. This Policy enters into force on the date stated in the header.
2. The Organiser reserves the right to amend the Policy; amendments take effect upon publication and communication to Participants.

3. Matters not regulated by this Policy are governed by Polish law, in particular the Civil Code and the Act on Electronic Services.
4. Any disputes arising in connection with the use of the VM shall be resolved by the court having jurisdiction over the Organiser’s registered office, unless mandatory provisions of law provide otherwise.
5. Starting to use the Virtual Machine constitutes acceptance of this Policy.

Version 1.0 – 20 June 2025