**Regulations for Access to the HPE Cluster Data Center at IUSS Pavia**

*The official and legally binding of the regulations is the one in Italian. This document is for informational purposes only and cannot be used for legal purposes*

## Art. 1. Scope of Application

These regulations apply to all physical and remote access to the HPE Cluster Data Center (hereinafter referred to as the "Data Center") of the Scuola Universitaria Superiore IUSS (hereinafter "IUSS").

## Art. 2. Access to the Data Center

Access to the Data Center facilities is restricted to personnel explicitly authorized by IUSS and Eucentre, as specified via pec exchange between the parties.

Remote access to the Data Center's compute nodes is provided trough a VPN connection, subject to the issuance of credentials. This access in conditional upon assignment to a Work Group by the designated Group Leader, and completion of a responsibility acceptance from the user.

Access to the virtualization nodes is reserved exclusively for system administrators for the purpose of managing virtual machines and related operations.

Access to individual virtual machines in granted via personal credentials.

Only individuals directly involved in projects defined by IUSS, Eucentre, or by officially affiliated institutions may submit access requests.

## 3. User Responsibilities

Authorized users must comply with security policies and ensure appropriate use of the resources.

Specifically, the user is fully responsible for proper use of their account, which is strictly personal and non-transferable. IUSS is held harmless from any misuse of the user's account, including any resulting civil or criminal liability.

Use of the Data Center for commercial purposes is permitted only up to a maximum of 20% of the total activity. Users are required to adhere to this limit and consult the relevant IUSS office beforehand for confirmation.

Users must promptly notify the competent office upon termination of their relationship with their home institution so that the account can be deactivated.

## 4. Security Policies

Data Center accounts are strictly personal. Shared use or transfer to third parties is prohibited.

Password changes are not permitted. Any loss of credentials must be reported immediately to the appropriate IUSS office.

Access to compute nodes is allowed solely for activities authorized by IUSS, as indicated in the responsibility acceptance form and upon inclusion in a HPC project.

Any unauthorized use will result in immediate access revocation, possible disciplinary actions under IUSS internal regulations, and, in serious cases, liability for any damage incurred by IUSS.

All general IUSS rules regarding data protection and confidentiality apply to use of the Data Center.

IUSS monitors all access activity and may request users to provide information regarding their usage.

## 5. Sanctions

Violations of usage rules and/or security policies will be subject to sanction by IUSS.

Depending on the severity of the violation, sanctions may range from a formal warning to revocation of credentials.

In most serious cases, IUSS reserves the right to take legal action before the appropriate civil and criminal authorities.