Workstation Security Policy

1. Overview

The aim of this acceptable use policy is not to restrict the usage of systems but to ensure that are not used in an illegal or damaging way.

Internet or intranet related systems, including, but not limited to workstations and network accounts belong to OVHCloud, and should only by used for business purposes.

Workstations (either fixed or mobile) are a preferred application access method for many employees located at OVHCloud facilities.This document describes required minimal security configurations for networks accounts and for all workstations connected and used in a production capacity on the OVHCloud network.

It is the user’s sole responsibility to know and apply the following policies. Information security begins at endpoint devices, and effective security involves the participation of all employees and affiliate of OVHCloud.

2. Purpose

The purpose of this policy is to provide workstation and network accounts security procedures that ensure information on workstations and the networks they operate on are safe and viable. Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity, and availability of information. This policy helps ensure that access to sensitive information is restricted to authorized users.

3. Scope

This policy applies to all OVHCloud staff and affiliate that use, configure, or support desktop workstations, and/or networks accounts.

4. Policy

Network account and computer workstation users shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access. The following procedures shall be in force to manage technical, physical, and administrative controls and safeguards:

A. PHYSICAL SAFEGUARDS

Physical access to workstations shall be restricted to authorized personnel and affiliate only. Employees and affiliates shall prevent unauthorized viewing of information on a screen by:

- Ensuring monitors are positioned away from public view
- If necessary, privacy screen filters or other physical barriers to prevent public viewing shall be installed
- Manually activating a password protected screen saver when staff leave their desk
- Exiting running applications and closing any open documents when leaving a workstation
- Ensuring workstations are logged off at the end of each business da

- Staff shall keep food and drink away from workstations in order to avoid accidental spills

Access to network account should only be done from a trusted system (work computer), and never from a personal or public system. The login information should not be saved in the web browser. The password used for the network account should only be used for that purpose and shall not be used in another account, whether personal or professional.

B. OPERATIONAL SAFEGUARDS

Employees and affiliates shall use workstations for authorized business purposes only and only approved personnel may install software on workstations. All sensitive information must be stored on network servers. Staff shall comply with all applicable policies and procedures related to desktop computing.

The only external devices that can be plugged in the computer (USB key, external disk, …) should only be those that are property of OVHCloud. In no case a devices coming from another source, whether know or unknown, should be plugged on the workstation.

Users should not use sharing files sites to share information with other within the company, and use only the dedicated system from the company.

Employees and affiliates must avoid downloading files from unknown sources, and shall be extremely careful when downloading a file from a known source as well.

C. MANAGEMENT AND ADMINISTRATION

OVHCloud maintenance team shall ensure that all workstations use a surge protector and/or a UPS battery backup. Workstations shall have all critical security updates and patches installed in a timely manner. The team will also provide users with necessary devices for their work, such as external devices for data storage.

OVHCloud network team shall ensure that all network accounts password are updated regularly, and that the network is safe to use for all employees and affiliates.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the OVHCloud. Satisfactory examples of evidence and compliance include:

- Spot user checks for compliance with general workstation computing policies
- Documented patch logs for workstations showing patches, dates, and systems installed
- Verification of UPS and/or surge protection installed on physical equipment
- Sport user checks for compliance with network accounts policies

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all OVHCloud staff and affiliates.

8. Policy Version History

Version	Date	Description	Approved By
1.0	18/04/2021	Initial Policy Drafted	Jon Smith
1.1	25/11/2021	Initial Policy updated with network account policies	Jon Smith