Cybersecurity Guidelines

Target group of the guideline

The following guideline concern all employees and affiliate of OVH Cloud. It is the user's sole responsibility to know and apply the guideline, and all employees and affiliates of OVH Cloud should read the guidelines carefully to ensure its full comprehension.

Introduction

Cybersecurity is a matter for everyone and effective security involves everyone participation. The document outlines guidelines for preserving: the security of the private data of the organization, the security of clients' data stored by OVH Cloud, the security of employees and affiliate data stored by the organization, the security of the technological infrastructure of OVH Cloud, and everything that could be at risk during a cybersecurity breach.

Physical security

Every employees and affiliate is encouraged to do is best in keeping their personal and work devices as protected as possible. Devices should not be left exposed or unattended; the devices need to be locked or turned off if it has to be left unattended. Stolen devices need to be reported as soon as possible to the IT team. All devices should be protected by a password.

Employees and affiliate should not plug in a devices from a unknown source in a device that contain sensible data.

Sensible information, including, but not limited to passwords, should not be displayed on the desk of employees, or in any place where it could be found by someone else.

Information security

Information system security

All employees have an access with login and password to the information system. Some affiliates have an access too, and are therefore asked to follow the same guidelines when using it.

Password guidelines

The employees and affiliate are given a temporary password at the creation of the account, that need to be changed at first connection. The new password needs to be at least 10 characters long, and should contains at least two of each elements of the following list: capital letters, lower-case letters, numbers and symbols.

The password should not contain personal information such a birthday date, anniversary, a relative or a pet name, etc.

The password need to be changed at least every two month, and needs to be changed every time it could have been compromised; for example, when a device is lost.

Login guidelines

Employees and affiliate are asked to login in the information system only though secure and private networks. They should also not save the password in the web browser.

Employees should also avoid login in front of an unauthorized person.

Workplace security

Organizational security

Data protection