OVHcloud 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 & data protection

When employees and affiliate works with IT assets, they should do their best to protect the information of OVH Cloud.

The guidelines for information security aim is to conserve the confidentiality, the integrity and the availabilty of the information, while ensuring that only authorized employees have access to information.

To ensure that, please report directly to IT Team if you find yourself able to access information your are not authorized to.

Information classification

Information can have three level of confidentiality : *secret, confidential, public.*

Public data is accessible to all amployees and affiliate and can be showed and shared to anyone in this group of person.

Confidential information is only accessible to a few affiliates and all employees. The list of affiliate authorized on confidential data is available on the information system.

Secret information can not be accessed by affiliates. The data can only be accessed through the information system and should not be shared; all employes that are authorized to access the information can do it from their account. If they do not find the information, you can help them access it by showing how to do so, or direct them to the IT Team to help them. The employees authorization is defined by : their seniority, the sector they are working in, and their position.

Employees and affiliates with lower authorization level should not access data their are not authorized for. Only administration can grant authorization to someone.

Data storage & GDPR

Users data collection on storage needs to follow GDPR, which mean:

- The data collected need to be used for explicit & transparent purposes
- The data should be accurate and kept up to data as much is possible
- The data should not be kept longer than necessary
- The data need to be kept safe and secure

The decision to store data should be considered carefully. If the data is used directly and will never be used again, it should not be stored.

When data is stored and is no more usefull for you or your departement, before deleting it you should considere :

- Asking other departement or employees if they still needs the data

- Communicate the decision with the IT Team, it a way that they can manage the back-up accordingly

Back-up of information and data

All information is backed up every 12h by the IT Team. If you need sensible data to be backed up immediately, you can contact the IT Team to do so.

The back up is only accessible by the administration and the head of the IT Team. For access, you should contact the IT Team so that they will upload the backup on the information system for you.

Data for users is also backed up, and when data is removed from the system it should also not remain on the backup. A user can ask for its data to be totally destroyed, and every backup needs to be updated accordingly. The deletion of data on the backup is the matter of the IT Team.

You should be carefull when deleting data from the information system when you are authorized to do.

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. It is better to not use words or expression either, even if you replace some letters by numbers.

Your password should also not be used for another account, whether personal or professional.

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.

All employees and affiliates need to use two factor authentication.

Login guidelines

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

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

Workplace security

There is no such things as a safe place when we talk about cybersecurity, and this is why employees and affiliates should still be cautious, even at their workplace.

Workstation security

Physical access to workstation from unauthorized person should be restricted.

All running application and open documents needs to be closed when leaving the workstation.

If the system appears to not be up-to data on the workstation :

- If possible, use another workstation which is up to date
- Warn the IT team and follow their instruction

Workstation should only be used for business related purposes.

Other threats

Employees and affiliates can face other threats as the workplace, such a phishing attempts, or other use of social engineering methods to extract sensible information. For that reason, employees and affiliates should follow theses guidelines :

- Always check the person from which the information is coming from, to ensure they are legitimate: name, email, role in the company, if it is logical that the information / instruction come from them
- Do not open links and attachments from unknown sources, and be careful even when the source is known: attachments should only be transferred through OVH cloud internal file sender, and the specific content behind a link should be explained
- Clickbait title (advices, offering prices, not stating the content clearly), grammar mistakes, weird phrasing can be give-aways from a malicious email

- If something does not seems safe, or if you have any doubt, please report it as soon as possible to the IT Team

Organizational security

- When receiving instruction / question, do not answer if you are not responsible of the matter
- If you are not authorized to give an information or to help someone, refer them to an authorized person
- Do not let someone else use your account or your workstation, because you could have different authorization
- If you need more authorization for a work: first, ask if you understood correctly what to do, and refer to your superior for further instructions