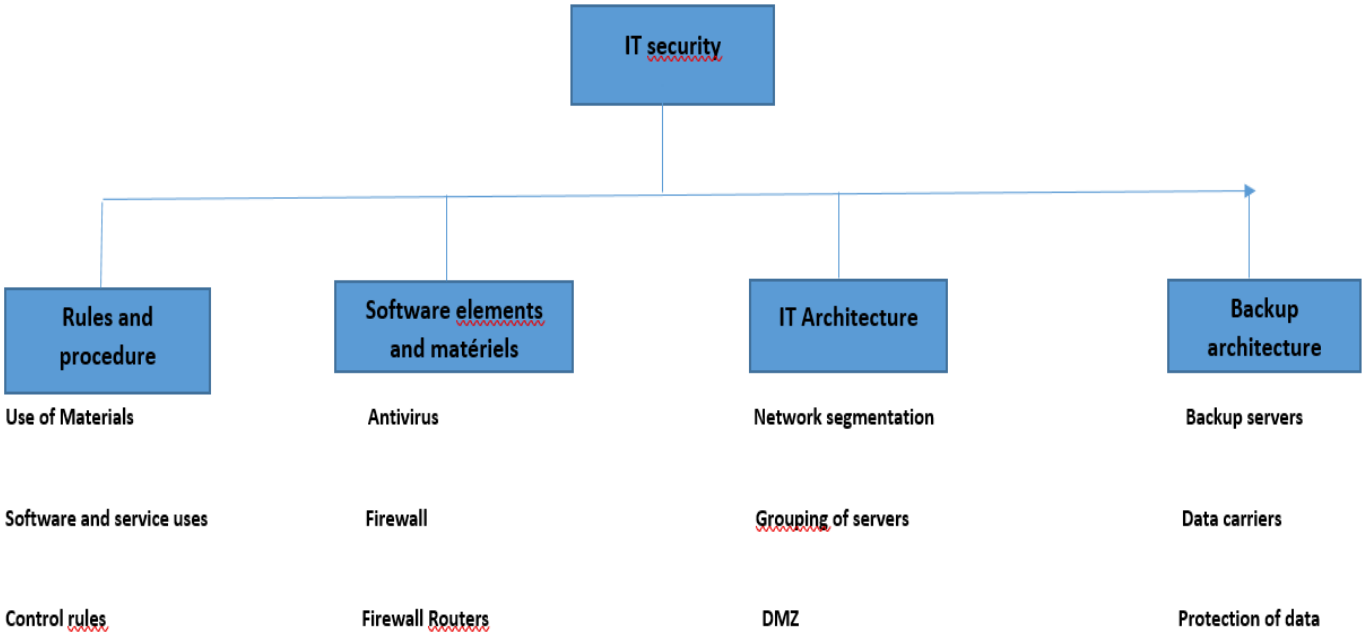
INFORMATION SECURITY POLICY

A) NETWORK SECURITY
   1- ACCESS RIGHTS
   2- IMPLEMENTATION OF GPOs
   3- ANTIVIRUS MANAGEMENT
   4- MESSAGING AND INTERNET MANAGEMENT
   5- TRAINING OF USERS

B) APPLICATION SECURITY
   1- ACCESS RIGHTS
   2- ENCRYPTION

C) DATA SAVING
   1- INTERNAL BACKUP
   2- REMOTE BACKUP

I) INFORMATION SECURITY POLICY



COMPUTER SECURITY ELEMENTS

A) NETWORK SECURITY

1- ACCESS RIGHTS

To implement our security policy, a domain has been created. The latter is managed by a domain controller. Access to data requires you to have identifiers (Login / password) to access a session and be able to find all the information to which this profile is entitled. This therefore allows us to track all user activities through log logs and to be able to control the flow and access to data. A series of shared drives are created, each mapped with the users who should have access to them as well as the permissions (read / write / not allowed).

The IT department delimits the restricted access areas and installs the security systems and the necessary equipment according to a threat and risk assessment (fire detection, extinguishers)

Management also ensures that the necessary measures are put in place to protect the equipment and the information it contains (access to the USB key disabled, access to the office restricted during each session, no authorization to administrative commands).

2- IMPLEMENTATION OF GPOs

Group policies are sets of settings that apply to users and computers. They make it easier to manage the security of one workstation or several workstations in a Domain. They allow, for example, to redirect the My Documents folder, to deploy Software according to the services of a company or to users. GPOs exist from the creation of a Domain, this is where the various operations of the domain are registered. There are two types when the domain is created. The GPOs set up in our case allow us to control the different profiles and their rights. Indeed, thanks to these GPOs, we are able to restrict access to certain workstation resources depending on the profiles. For example, not all call center sessions have the right to install third-party software on workstations. Several GPOs have been set up and are classified according to departments.

3- ANTIVIRUS MANAGEMENT

An antivirus server has been set up in the network. Indeed on this server is installed ESET ANTIVIRUS which performs regular updates by connecting to the ESET server from the Internet. It is also installed on all workstations in the company (Production, Administration). Given the security policy in place, they carry out their updates directly from the local server and thus protect us from the risk of viral or worm infection.
In case of infection, a full scan of all disks is immediately performed to remove the threat as soon as possible.

4- MAIL AND INTERNET MANAGEMENT

Management ensures that measures are put in place to prevent SPAM, inform and supervise staff on the use of electronic mail and the Internet.

Internet access is only permitted by administrative staff and opening email attachments is done with care to limit the execution of malicious code. An Internet access schedule is also defined to better manage the QOS.

5- TRAINING OF USERS

The objective of user training is to make them independent in the use of tools and applications that are useful for performing their tasks in the company. For each new application developed by the department, operational training is scheduled and a user manual is provided. The other part of this training consists of raising awareness of the threats related to the security of the internal network (use of USB keys, use of sessions, etc.) training or action to be taken in the event of an incident related to personal safety .

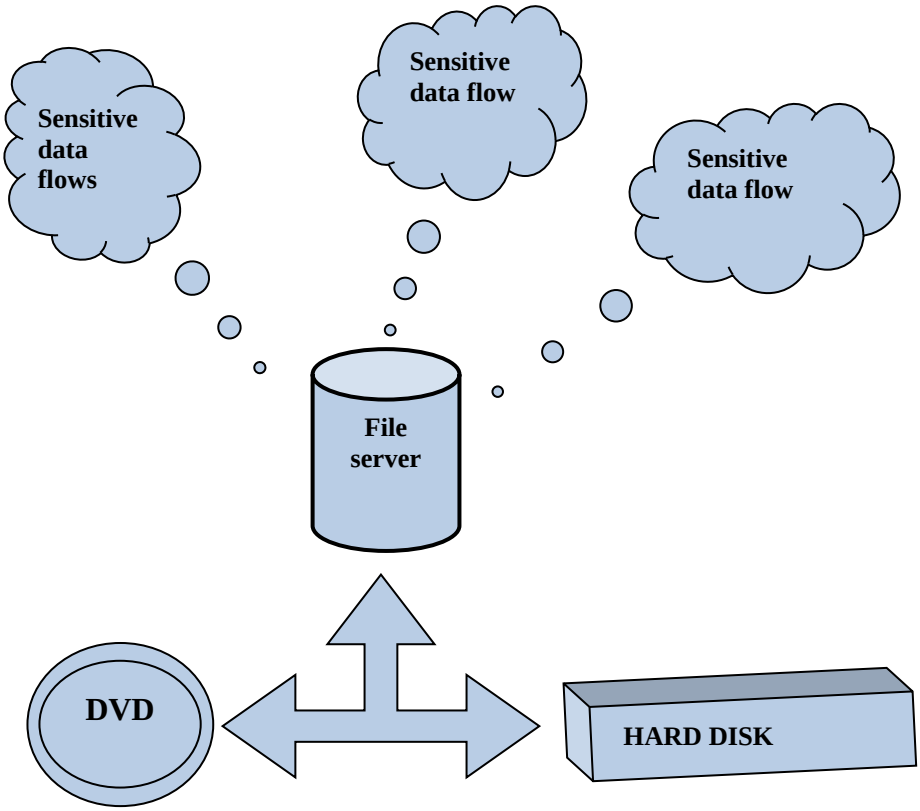
B) APPLICATION SECURITY

1- ACCESS RIGHTS

Logon credentials provide access to basic resources (readers only), and they do not guarantee access to the applications necessary to conduct business. Access rights are used to define, locate and limit user actions on well-defined functionalities in an application. Depending on the type of applications, these rights may vary but, except in exceptional cases, they will include a right to administer the application and a right of access to the main functionalities for the users for whom the application is intended. For databases, the definition of rights is up to the CIO who assigns them to administrators or developers according to their profile.

2- ENCRYPTION

Encryption is a process designed to protect the confidentiality of certain application data. The application specifications must express the need to make certain sensitive information confidential so that in the event of theft, this data cannot be used.
The method



1- REMOTE BACKUP

As for the external data backup, it consists in depositing certain data on a remote space. In our case, this is a space at OVH (On Vous Héberge) accessible via an FTP link or an FTP client. This space is secure and sometimes allows us to keep certain data such as updates of certain business applications, backups of certain applications and website.