

# GUIDELINE FOR A HEALTHY INFORMATION SYSTEM

*STRENGTHEN INFORMATION SYSTEM SECURITY IN 42 MEASURES*

---





## FOREWORD

With its first edition released in January 2013, the Guideline for a Healthy Information System guide published by the national cybersecurity agency of France (Agence nationale de la sécurité des systèmes d'information or ANSSI) is for public or private organizations equipped with an IT team or professionals whose mission is to ensure information system (IS) security. It stems from the observation that if the measures set out had been applied by the organizations concerned, the majority of cyberattacks which required intervention of the agency could have been avoided.

This new edition has been updated as regards both new and growing technologies and practices, which must be addressed in terms of security (mobile working, separation of uses, etc.) and also the introduction of tools (indicators of a standard or strengthened level) to enlighten the reader in the appreciation of the specified measures. Although the purpose of this guide is not information security as such, applying the proposed measures maximises the security of the information system, the information cradle of your organization.

IS security is no longer optional. To this end, IS security stakes must come to occupy a similar level as the economic, strategic and even image concerns of decision makers. By contextualising the need, giving a reminder of the intended aim and responding to it by applying the corresponding concrete measure, this document is a roadmap which is in the interest of all organizations aware of the value of their data.

# CONTENTS

## FOREWORD HOW TO USE THE GUIDE

---

- I** - RAISE AWARENESS AND TRAIN - *P.4*
  - II** - KNOW THE INFORMATION SYSTEM - *P.8*
  - III** - AUTHENTICATE AND CONTROL ACCESSES - *P.13*
    - IV** - SECURE THE DEVICES - *P.20*
    - V** - SECURE THE NETWORK - *P.26*
    - VI** - SECURE ADMINISTRATION - *P.36*
    - VII** - MANAGE MOBILE WORKING - *P.40*
  - VIII** - KEEP THE INFORMATION SYSTEM UP TO DATE - *P.45*
    - IX** - SUPERVISE, AUDIT, REACT - *P.48*
    - X** - TO GO EVEN FURTHER - *P.55*
- 

## MONITORING TOOL BIBLIOGRAPHY

## HOW TO USE THE GUIDE

This document includes 42 simple security measures. Each of them is important and you can definitely consider each one independently of each other to improve your security level on some specific points.

However, we advise you to use this guide as a basis to define an action plan:

1. Start with establishing an assessment for each of the rules thanks to the monitoring tool which is to be found in the appendix of this document. For each rule, determine if your organization has achieved the standard level and, if required, the strengthened level.
2. If you are unable to do this assessment because you are not sufficiently familiar with your information system, do not hesitate to ask for assistance from a specialist to carry out an assessment and ensure a basic level of security. (Worth reading: ANSSI-CGPME, *Guide des bonnes pratiques de l'informatique* (IT good practice guide), March 2015).
3. From this assessment established at this initial stage, target the rules for which you have not yet reached "standard" level as a priority, in order to define an initial action plan. If the measures of this guide must be applied in the context of a reference document published by ANSSI, unless mentioned explicitly, this concerns the "standard" level measures.
4. When you have reached the "standard" level everywhere, you can define a new action plan aiming for the "strengthened" level for the rules concerned.



**RAISE AWARENESS AND TRAIN**

# 1

## Train the operational teams in information system security

### / STANDARD

The operational teams (network, security and system administrators, project managers, developers, chief information security officer (CISO)) have special access to the information system. They can, inadvertently or through not understanding the consequences of certain practices, carry out operations creating vulnerabilities.

We can cite for example, granting accounts with too many privileges in relation to the task to be carried out, the use of personal accounts to carry out services or periodical tasks, or even choosing passwords that are not sufficiently robust granting access to privileged accounts.

The operational teams, to comply with information system security accepted practice, must therefore undertake - upon taking on their role and, subsequently, at regular intervals - training on:

- > the legislation in effect;
- > the main risks and threats;
- > security maintenance;
- > authentication and access control;
- > the detailed configuration and hardening of systems;
- > network partitioning;
- > and logging.

This list must be specified according to the employee's job , considering aspects such as security integration for project managers, secure development for developers, the security reference documents for ISSMs, etc.

Moreover, it is necessary to mention specific clauses in service agreements in order to guarantee regular training in information system security for external staff and especially outsourcers.

# 2

## Raise users' awareness about basic information security

### / STANDARD

Each user is a part of the information system chain. To this end, as he enters the organization, he must be informed of the security stakes, the rules to respect and the proper behaviour to adopt in terms of information system security by awareness raising and training actions.

These actions must be regular and adapted to the users targeted. It may take different forms (emails, displays, meetings, dedicated intranet space, etc.) and, as a minimum, deal with the following issues:

- > the objectives and stakes that the organization encounters in terms of information system security;
- > the information considered as sensitive;
- > the regulations and legal obligations;
- > the rules and security instructions governing daily activity: adhering to the security policy, not connecting personal devices to the network of the organization, not divulging passwords to a third party, not reusing professional passwords in the private sphere or the other way round, reporting suspicious events, etc.;
- > the means available and involved in computer security: systematically locking the session when the user leaves his device, password protection tool, etc.

### / STRENGTHENED

To strengthen these measures, the creation and signature of an IT resource charter specifying the rules and instructions that must be adhered to by users may be considered.

ANSSI, *Charte d'utilisation des moyens informatiques et des outils numériques - Guide élaboration en 8 points clés pour les PME et ETI (IT and digital tools user charter)*, guide, June 2017



# 3

## Control outsourced services

### / STANDARD

When an organization wants to outsource its information system or data, it must assess, in advance, the risks specific to outsourced services (controlling the information system, remote actions, shared hosting, etc.) in order to take into account the needs and suitable security measures when creating the requirements applicable to the future service provider.

The information security system risks inherent in this type of approach may be linked to the context of the outsourcing operation, but also deficient or incomplete contractual specifications.

Therefore, in order to run smoothly the operations, it is important to:

- > carefully study the offers' conditions, the option of adapting them to the specific needs and the limits of the service provider's responsibility;
- > impose a list of specific requirements on the service provider: contract reversibility, the carrying out of audits, backup and data recovery in a
- > standardised open format, security maintenance over time, etc.

To formalise these commitments, the service provider will provide the customer with a security insurance plan detailed in the bid. This is a contractual document describing all of the specific measures that the applicants commit to implementing in order to guarantee the security requirements specified by the organization are met.

The use of digital solutions or tools (hosted in the Cloud for example) is not considered here as it comes under the area of managed services and, moreover, is not advisable when processing sensitive data.

ANSSI, *Guide de l'externalisation – Maîtriser les risques de l'infogérance (Outsourcing guide – controlling the risks of managed services)*, guide, December 2010



**KNOW THE INFORMATION SYSTEM**

# 4

## Identify the most sensitive information and servers and maintain a network diagram

### /STANDARD

Each organization has sensitive data. This data can be on its own activity (intellectual property, expertise, etc.) or its customers, individuals or users (personal data, contracts, etc.). In order to effectively protect your data, identifying it is essential.

From this list of sensitive data, it will be possible to determine in which areas of the information system it is located (databases, file sharing, workstations, etc.). These components correspond to the servers and critical devices of the organization. To this end, they must be subject to specific security measures that may concern backup, logging, access, etc.

Therefore, this involves creating and maintaining a simplified network diagram (or mapping) representing the different IP areas and the associated addressing plan, the routing and security devices (firewall, application relays, etc.) and the networks with the outside (Internet, private networks, etc.) and partners. This diagram must also be able to locate the servers holding the entity's sensitive information.

# 5

## Have an exhaustive inventory of privileged accounts and keep it updated

### /STANDARD

Accounts benefiting from specific permissions are preferred targets for the attackers who want to obtain as wide an access as possible to the information system. They must therefore be subject to very specific attention. This involves carrying out an inventory of these accounts, updating it regularly and entering the following informations into it:

- > users with an administrator account or higher rights than those of a standard user in the information system;
- > users with rights enough to access the work folders of top managers or all users;
- > users using an unmanaged workstation which is not subject to the security measures detailed in the general security policy of the organization.

Carrying out a periodical review of these accounts is strongly recommended in order to ensure that the accesses to sensitive items (notably the work folders and electronic mailboxes of top managers) are controlled. These reviews will also be the opportunity to remove access rights that have become obsolete following the departure of a user, for example.

Lastly, defining and using a simple, clear nomenclature to identify system accounts and administration accounts is desirable. This will make review and intrusion detection easier.

# 6

## Organise the procedures relating to users joining, departing and changing positions

### /STANDARD

The staff of an organization, whether public or private, is constantly changing : arrivals, departures, internal mobility. Therefore it is necessary to update the rights and accesses to the information system in accordance with these developments. It is essential that all of the rights granted to an individual are revoked when he or she leaves or changes position. The arrival and departure procedures must therefore be defined, in accordance with the human resources department. They must, as a minimum, take into account:

- > the creation and deletion of IT accounts and their corresponding mailboxes;
- > the rights and accesses to grant to, or remove from, an individual whose role changes;
- > the management of physical accesses to premises (granting and return of badges and keys, etc.);
- > the allocation of mobile devices (laptops, USB sticks, hard drives, smart-phone, etc.);
- > the management of sensitive documents and information (transferring passwords, changing passwords or codes in existing systems).

### /STRENGTHENED

The procedures must be formalised and updated according to the context.

# 7

## Only allow controlled devices to connect to the network of the organization

### /STANDARD

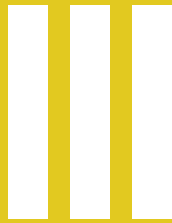
To guarantee the security of the information system, the organization must control the devices which connect to it, each one being a potentially vulnerable entry point. Personal devices (laptops, tablets, smartphones, etc.) are, by definition, difficult to control since it is the users who decide on their level of security. In the same way, the security of visitors' devices is completely out of the organization's control.

Only the connection with terminals managed by the entity must be authorised over its different access networks, whether wired or wireless. This recommendation, above all of an organisational nature, is often perceived as unacceptable and even retrograde. However, unless this is adhered to, the task of a hacker is made very much easier by making an organization's network vulnerable.

Raising users' awareness must therefore be accompanied by pragmatic solutions responding to their needs. For example, the provision of a Wi-Fi network with dedicated SSID for personal and visitor devices.

### /STRENGTHENED

These developments can be supplemented by technical measures such as the authentication of devices on the network (for example thanks to 802.1X standard or an equivalent).



**AUTHENTICATE AND CONTROL ACCESSES**

# 8

## Identify each individual accessing the system by name and distinguish the user/administrator roles

### /STANDARD

In the event of an incident, in order to facilitate the attribution of an action within the information system or the identification of possible compromised accounts easier, access accounts must be nominative.

The use of generic accounts (e.g : *admin*, *user*) must be marginal and they must be able to be associated with a limited number of individuals.

Of course, this rule does not stop you from retaining service accounts attributed to an IT process (e.g : *apache*, *mysqld*).

In any event, generic and service accounts must be managed according to a policy that is at least as stringent as the one for nominative accounts. Moreover, a nominative administration account, different from the user account, must be attributed to each administrator. The usernames and authentication secrets must be different (e.g : *pmartin* as a username, *adm-pmartin* as an admin username). This admin account, having more privileges, must be exclusively dedicated to administration actions. Furthermore, it must be used in environments dedicated to administration in order that no connection traces or password hashes are left in a more exposed environment.

### /STRENGTHENED

As soon as possible, the logging linked to accounts (e.g.: list of successful/failed connections) must be activated.



# 9

## Allocate the appropriate rights to the information system's sensitive resources

### /STANDARD

Some of the system's resources can be a source of invaluable information from the hacker's point of view (folders containing sensitive data, databases, mailboxes, etc.). It is therefore essential to establish an accurate list of these resources and for each of them:

- > define which group can have access to them;
- > strictly control access, by ensuring that users are authenticated and are part of the target group;
- > avoid their circulation and duplication to uncontrolled areas or areas subject to a less strict access control.

For example, the folders of administrators bringing together various pieces of sensitive information must be subject to specific access control. The same goes for sensitive information present on network shares: exports of configuration files, information system technical documentation, business databases, etc. A regular review of the access rights must, moreover, be carried out, in order to identify any unauthorised access

# 10

## Set and verify rules for the choice and size of passwords

### /STANDARD

ANSSI sets out a collection of rules and best practices in terms of the choice and size of passwords. The most critical one is to make users aware of the risks involved in choosing a password that is too easy to guess, and even the risks of reusing the same password from one application to another, especially for personal and professional mailboxes.

To supervise and confirm that these choice and size rules are being applied, the organization may use different measures, including:

- > blocking accounts following several failed logins;
- > deactivating anonymous login options;
- > using a password robustness checking tool.

In advance of such procedures, communication aiming to explain the reason for these rules and raise awareness of their importance is fundamental.

ANSSI, *Recommandations de sécurité relatives aux mots de passe* (Security recommendations relating to passwords), technical note, June 2012

# 11

## Protect passwords stored on systems

### /STANDARD

The complexity, the diversity and even the infrequent use of some passwords may encourage their storage on a physical (memo or post-it) or digital (password files, sending an email to yourself, recourse to "Remember password" buttons) medium in the event a password is lost or forgotten.

Yet passwords are a preferred target for hackers wanting to access the system, whether it is following a theft or the possible sharing of a storage medium. This is why they must be protected by secure solutions, the best of which are using a digital safe and using encryption mechanisms.

Of course, the password chosen for this digital safe must respect the rules set out previously and be memorised by the user, who only has to remember this password.

# 12

## Change the default authentication settings on devices and services

### /STANDARD

It is essential to consider that the default settings of the information systems are known by the hackers, even if these are not known to the general public. These settings are (too) often trivial (password the same as the username, not long enough or common to all the devices and services for example) and are often easy to obtain by hackers capable of pretending to be a legitimate user.

The default authentication settings of the components of the system must therefore be changed when they are set up and, in terms of passwords, be in accordance with the previous recommendations in terms of choice, size and storage.

If changing a default password is impossible due, for example, to a password or certificate being "hardcoded" onto a device, this critical problem must be raised with the product supplier so that it can correct this vulnerability as fast as possible.

### /STRENGTHENED

In order to limit the consequences of a compromise, it is, moreover, essential, after changing the default authentication settings, to renew them regularly.

# 13

## Prefer a two-factor authentication when possible

### /STANDARD

The implementation of a two-factor authentication is strongly recommended, requiring the use of two different authentication factors from among the following:

- > something I know (password, unlock pattern, signature);
- > something I have (smart card, USB token, magnetic card, RFID, a phone to receive an SMS);
- > something I am (a digital fingerprint).

### /STRENGTHENED

Smart cards must be encouraged or, by default, one-time passwords with a physical token. Encryption operations implemented with two-factor authentication generally offer good security results.

Smart cards can be more complex to implement as they require an adapted key management structure. However, they have the advantage of being re-usable for various purposes: encryption, message authentication, authentication on the workstation, etc.

# IV

**SECURE THE DEVICES**

# 14

## Implement a minimum level of security across the whole IT stock

### /STANDARD

Depending on his level of IT security practices, the user, a great deal of the time, is the first port of call for hackers trying to enter the system. It is therefore fundamental to implement a minimum level of security across the entire IT stock of the organization (user devices, servers, printers, phones, USB peripherals, etc.) by implementing the following measures:

- > limit the applications installed and optional modules in web browsers to just what is required;
- > equip users' devices with an anti-virus and activate a local firewall (these are often included in the operating system);
- > encrypt the partitions where user data is stored;
- > deactivate automatic executions (autorun).

In the event of a necessary exception from the general security rules applicable to devices, these devices must be isolated from the system (if it is impossible to update certain applications for interoperability reasons for example).

### /STRENGTHENED

Data vital to the proper business of the organization that is held on users' devices and servers must be subject to regular backups and stored on disconnected devices, and its restoration must be tested periodically. An increasing number of small organisations are subject to attacks which make their data unavailable (for example demanding, in exchange for returning the data, the payment of a significant amount of money (ransomware)).

# 15

## Protect against threats relating to the use of removable media

### /STANDARD

Removable media can be used to spread viruses, steal sensitive and strategic information or even compromise the organization's network. Such attacks can have disastrous consequences for the activity of the organisation targeted.

Although it is not a matter of completely prohibiting the use of removable media within the organization, it is nevertheless necessary to deal with these risks by identifying adequate measures and by raising users' awareness to the risks that these media can carry.

It is advisable to prohibit the connection of unknown USB sticks (collected in a public area for example) and to reduce, as much as possible, the use of uncontrolled sticks (the origin of which is known but not the integrity) on the information system, or at least have their content examined by the workstation's anti-virus.

### /STRENGTHENED

On user devices, using solutions able to block the execution of programs on removable media (for example Applocker on Windows or noexec assembly options on Unix) is recommended.

At the end of the removable media's life span, it will be necessary to implement and respect a strict disposal procedure which may extend to their secure destruction, in order to limit the leaking of sensitive information.

ANSSI, *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows* (Recommendations for the implementation of a software restriction policy in Windows), technical note, December 2013

ANSSI, *Recommandations de configuration d'un système GNU/Linux* (Configuration recommendations for a GNU/Linux system), technical note, January

2016



# 16

## Use a centralised management tool to standardise security policies

### /STANDARD

The information system's security relies on the security of the weakest link. It is therefore necessary to standardise the management of security policies applying across the entire IT stock of the organization.

Applying these policies (managing passwords, restricting logins on certain sensitive devices, configuring web browsers, etc.) must be simple and quick for administrators, with a view to facilitate the implementation of counter measures in the event of an IT crisis.

To do this, the organization may deploy a centralised management tool (for example Active Directory in the Microsoft environment) into which it is possible to include as many IT devices as possible. Workstations and servers are concerned by this measure, which may require upstream harmonization work in matter of hardware and operating systems selection.

Therefore, hardening policies for the operating system or applications may easily be applied from a central point while favouring the expected responsiveness in the event reconfiguration is required.

*ANSSI, Recommandations de sécurité relatives à Active Directory (Security recommendations relating to Active Directory), technical note, September 2014*

# 17

## Activate and configure the firewall on workstations

### /STANDARD

After having succeeded in taking control of a workstation (due, for example, to a vulnerability of the web browser), a hacker will often seek to spread his intrusion to other workstations and, ultimately, access users' documents.

In order to make this sideways movement from the hacker more difficult, it is necessary to activate the local firewall of workstations thanks to built-in (local Windows firewall) or specialised software.

Flows from device to device are very rare in a traditional office network: files are stored on file servers, applications are accessible on business servers, etc.

### /STRENGTHENED

The most simple filter consists of blocking access by default to administration ports from workstations (TCP 135, 445 and 3389 ports in Windows, TCP 22 port in Unix), except from explicitly identified resources (administration and user assistance devices, possible management servers requiring access to network shares on devices, etc.).

An analysis of useful incoming flows (administration, infrastructure software, particular applications, etc.) must be carried out to define the list of authorisations to configure. It is preferable to block all of the flows by default and only authorise the necessary services from the corresponding devices («white list»).

The firewall must also be configured to log the blocked flows and therefore identify the application configuration errors or intrusion attempts.

# 18

## Encrypt sensitive data sent through the Internet

### /STANDARD

The Internet is a network from which it is almost impossible to obtain guarantees as to the way that data will take when you send it through this medium. It is, therefore, entirely possible that a hacker will be on the pathway of data travelling between two correspondents.

All the data sent by email or uploaded to online hosting tools (Cloud) is therefore vulnerable. Therefore, its systematic encryption must be undertaken before sending it to a correspondent or uploading it.

Passing on confidential information (password, key, etc.) that is therefore able to decrypt data, if required, must be carried out by a trusted channel or, failing that, a different channel from the data transmission channel. Therefore, although the encrypted data is sent by mail, handing over the password by hand or, failing that, over the phone must be favoured.

**V**

**SECURE THE NETWORK**

# 19

## Segment the network and implement a partitioning between these areas

### /STANDARD

When the network is "flat", without any partitioning mechanism, each device in the network can access any other device. If one is compromised all of the connected devices are therefore in jeopardy. A hacker can therefore compromise a user's device and then, moving around from device to device, find a way to critical servers.

Therefore it is important, from the network architecture's design, to work through segmentation into areas made up of systems with uniform security needs. You may, for example, separately group infrastructure servers, business servers, user workstations, administrator workstations, IP phones, etc.

One area is therefore characterised by dedicated VLANs and IP subnetworks or even by infrastructures dedicated according to their criticality. Therefore, partitioning measures such as an IP filter with the help of a firewall can be implemented between the different areas. Specifically, you will ensure that the devices and flows associated with administration tasks are segregated as far as possible.

For networks for which subsequent partitioning would not be easy, integrating this approach in any new network extension or when devices are changed is recommended.

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu* (Recommendations for setting out a network filter policy for a firewall), technical note,

March 2013

## 20

Ensure the security of  
Wi-Fi access networks and  
that uses are separated

## /STANDARD

The use of Wi-Fi in a professional environment is now widespread, yet it still presents very specific security risks: poor guarantees in terms of availability, no control over the coverage area which can lead to an attack out of the geographical scope of the organization, default configuration of access points that are not secure by design, etc.

The network architecture segmentation must be able to limit the consequences of intrusion by radio access up to a given perimeter of the information system. The flows coming from devices connected to the Wi-Fi access network must therefore be filtered and restricted to just the necessary flows.

Furthermore, it is important to give priority to the use of robust encryption (WPA2 mode, AES CCMP algorithm) and centralised authentication, if possible through client certificates for devices.

Protecting the Wi-Fi network with a single and shared password is not advisable. However, if this is inevitable, it must be complex and its renewal must be planned, but under no circumstances must be transmitted to unauthorized third parties.

Moreover, access points must be administrated in a secure way (e.g.: dedicated interface, changing the default administrator password).

Finally, all Wi-Fi connection from staff or visitor terminals (laptops, smartphones) must be separate from Wi-Fi connections from the organization's devices (e.g.: distinct SSID and VLAN, dedicated internet access).

ANSSI, *Recommandations de sécurité relatives aux réseaux Wi-Fi* (Security recommendations relating to Wi-Fi networks), technical note, September 2013

# 21

## Use secure network protocols when they exist

### /STANDARD

Although security is no longer optional today, this has not always been the case. This is why numerous network protocols had to evolve to integrate this component and respond to the confidentiality and integrity requirements that exchanging data requires. Secure network protocols must be used as soon as possible, whether on public networks (the Internet for example) or on the organization's internal network.

Although it may be difficult to provide an exhaustive list, the most common protocols rely on the use of TLS and are often identifiable by the addition of the letter "s" (for secure) in the protocol acronym. As an example HTTPS for web browsing or IMAPS, SMTPS or POP3S for email.

Other protocols were designed securely from their creation to replace prior, insecure protocols. As an example SSH (Secure SHell) which came to replace the TELNET and RLOGIN historic communication protocols..

ANSSI, *Recommandations pour un usage sécurisé d'[OPEN] SSH* (Recommendations for secure use of [OPEN] SSH), technical note, August 2016

# 22

## Implement a secure access gateway to the Internet

### /STANDARD

Implement a secure access gateway to the Internet : websites hosting malware, the downloading of "infected" files and, consequently, the possibility of devices being compromised, leaking of sensitive data, etc. To secure this use, it is therefore essential that the users' devices do not have direct network access to the Internet.

This is why it is advisable to implement a secure Internet access gateway, including, as a minimum, a firewall as close to the Internet access as possible to filter the connections and a proxy server with different security mechanisms. This ensures users are authenticated and requests are logged.

### /STRENGTHENED

Additional mechanisms on the proxy server may be activated depending on the organization's needs: anti-virus analysis of the content, filtering by URL categories, etc. Security maintenance of the gateway's components is essential, it must therefore follow defined procedures. Depending on the number of employees and the availability requirement, these devices may be redundant.

Moreover, for user devices, the direct DNS resolutions of public domain names will be, by default, deactivated, as they are delegated to the proxy server.

Lastly, it is strongly recommended that mobile devices establish a prior secure connection to the organization's information system to browse the web securely through the gateway.



# 23

## Segregate the services visible from the Internet from the rest of the information system

### /STANDARD

An organization can choose to host internally services visible on the Internet (website, email server, etc.). In light of the development and improvement of cyberattacks online, it is essential to guarantee a high level of protection for this service with the competent administrators, available and continuously trained (up to date in terms of technology). Otherwise, recourse to outsourced hosting with professionals is to be favoured.

Furthermore, the web hosting infrastructures must be physically segregated from all the information system infrastructure, which is not designed to be visible from the Internet.

Lastly, it is advisable to implement an interconnection infrastructure for these services with the Internet, able to filter the flows linked to services differently from the other flows of the organization. It also concerns ensuring incoming flows go through a reverse proxy server with different security mechanisms.

ANSSI, *Guide de définition d'une architecture de passerelle d'interconnexion sécurisée* (Definition guide for secure gateway interconnection architecture), technical note, December 2011

ANSSI, *Maîtriser les risques de l'infogérance* (Controlling the risks of managed services), guide, December 2010

# 24

## Protect your professional email

### /STANDARD

Email is the main infection vector for a workstation, whether it is opening attachments containing malware or a misguided click on a link redirecting towards a site that is, itself, malicious.

Users must be especially aware of this issue: is the sender known? Is information from him or her expected? Is the proposed link consistent with the subject mentioned? If any doubt, checking the message authenticity by another channel (telephone, SMS, etc.) is required.

To protect against scams (e.g.: a fraudulent transfer request seeming to come from a manager), organisational measures must be strictly applied.

Moreover, the redirection of professional messages to a personal email must be prohibited as it may constitute an irremediable information leak from the organization. If necessary, controlled and secure methods for remote access to professional email must be offered.

Whether the organization hosts or has their email system hosted, it must ensure:

- > that it has an anti-virus analysis system upstream of the mailboxes of users to prevent the receipt of infected files;
- > that it has activated TLS encryption for exchanges between email servers (from the organization or public) as well as between the user devices and servers hosting the mailboxes.

---

**/STRENGTHENED**

Not directly exposing the mailbox servers to the Internet is preferable. In this case, a relay server dedicated to send and receive messages must be implemented in case the Internet is cut off.

While spam - whether malicious or not - accounts for the majority of email exchanges on the Internet, the deployment of an anti-spam service must be able to remove this source of risks.

Finally, the email administrator will ensure the implementation of authenticity verification mechanisms and the correct configuration of public DNS records linked to its email infrastructure (MX, SPF, DKIM, DMARC).

# 25

## Secure the dedicated network interconnections with partners

### /STANDARD

For operational needs, an organization can be required to establish a dedicated network interconnection with a supplier or customer (e.g.: managed services, electronic data interchange, financial flows, etc.)

This interconnection can be done by a link to a private network of the organization or directly online. In the latter case, it is advisable to establish a site to site tunnel, ideally IPsec, adhering to ANSSI's recommendations.

The partner is, by default, considered as unsafe, so it is essential to carry out IP filtering with the assistance of a firewall as close as possible to the flows' entrance into the organization's network. The flow matrix (incoming and outgoing) must be strictly reduced to the operational need, maintained over time and the devices' configuration must be in accordance with it.

### /STRENGTHENED

For organizations with more demanding security needs, it will be advisable to ensure that the IP filtering device for partner connections is dedicated to this use. The addition of an intrusion detection device may also be considered as a good practice.

Moreover, knowing an up-to-date point of contact for the partner is necessary to be able to react in the event of a security incident.

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau* (Security recommendations relating to IPsec for the protection of network flows), technical note, August 2015

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu* (Recommendations for setting out a network filter policy for a firewall), technical note, March 2013

# 26

## Control and protect access to the server rooms and technical areas

### /STANDARD

Physical security mechanisms must be a key part of information systems security and be up to date to ensure that they cannot be bypassed easily by a hacker. It is, therefore, advisable to identify the suitable physical security measures and to raise users' awareness continuously of the risks caused by bypassing these rules.

Access to server rooms and technical areas must be controlled with the assistance of locks or access control mechanisms such as badges. The unaccompanied access of external service providers to sever rooms and technical areas must be prohibited, except if it is possible to strictly monitor the access and limit it to given time intervals. A regular review of the access rights must be carried out, in order to identify any unauthorised access.

When an employee leaves or there is a change of service provider, the access rights must be withdrawn or the access codes changed.

Finally, the network sockets in areas open to the public (meeting room, reception hall, corridors, etc.) must be restricted or deactivated in order to stop a hacker easily gaining access to the company's network.

# VI

**SECURE ADMINISTRATION**

# 27

## Prohibit Internet access from devices or servers used by the information system administration

### /STANDARD

A workstation or a server used for administration actions must, under no circumstances, have access to the Internet, due to the risks that web browsing (websites containing malware) and email (potentially infected attachments) bring to its integrity.

For other administrator uses requiring the Internet (viewing documentation online, their email, etc.), it is advisable to provide them with a separate workstation. Failing this, access to a remote virtual infrastructure for office applications from an admin device is possible. The reverse, consisting of providing remote access to an admin infrastructure from an office device, is not advisable as it can lead to a privilege elevation in the event admin authenticators are recuperated.

### /STRENGTHENED

Concerning software updates for administrated devices, they must be collected from a safe source (the site of the publisher for example), tested then transferred to a device or server used for administration and not connected to the Internet. This transfer can be carried out on a dedicated removable medium.

For organizations wishing to automate certain tasks, the implementation of secure interchange area is advisable.

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information* (Recommendations relating to the secure administration of information systems), technical note, February 2015

# 28

## Use a dedicated and separated network for information system administration

### /STANDARD

An administration network interconnects, among others, the administration devices or servers and the device administration interfaces. Within the logic of segmentation for the organization's global network, it is essential to specifically segregate the administration network from the user office network, to prevent any intrusion by redirection from a user device to an administration resource.

Depending on the organization's security needs, it is advisable:

- > to firstly favour a physical partitioning of networks as soon as this is possible, as this solution can represent significant costs and deployment time; **/STRENGTHENED**
- > failing this, to implement a logical cryptographic partitioning relying on the implementation of IPsec tunnels. This allows for assurance over the integrity and confidentiality of data carried in the administration network over the user office network; **/STANDARD**
- > as a minimum, implement logical partitioning using VLAN. **/STANDARD**

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information* (Recommendations relating to the secure administration of information systems), technical note, February 2015



# 29

## Reduce administration rights on workstations to strictly operational needs

### /STANDARD

Numerous users, including at the top management level, are tempted to ask their IT department to be able to provide them, in line with their personal use, with higher privileges on their workstations: installation of software, system configuration, etc. By default, it is recommended that an information system user, whatever his responsibility level and allocations, should not have administration privileges on his workstation. This measure, which appears restrictive, aims to limit the consequences of malicious executions from malware. The availability of a well-rounded application store, validated by the organization from the security point of view, will be able to respond to the majority of needs.

Consequently, only administrators responsible for the administration of workstations must have these rights during their interventions.

If delegating privileges to a workstation is really necessary to respond to a one-off need from the user, it must be monitored, for a limited time, and be withdrawn afterwards.

# VII

**MANAGE MOBILE WORKING**

# 30

## Take measures to physically secure mobile devices

### /STANDARD

Mobile devices (laptops, tablets and smartphones) are, naturally, exposed to loss and theft. They may contain sensitive information for the organization, locally, and constitute an entry point to wider resources of the information system. Beyond the minimal application of the organization's security policies, specific security measures for these devices must therefore be provided.

First and foremost, users' awareness must be raised to increase their level of vigilance during their trips and keep their devices within sight. Any organization, even a small sized one, may be the victim of a cyberattack. Consequently, when mobile, any device becomes a potential or even favoured target.

It is recommended that mobile devices are as ordinary as possible, avoiding any explicit mention of the organization they belong to (by displaying a sticker with the colours of the organization for example).

To avoid any indiscretion during journeys, especially on public transport or in waiting areas, a privacy filter must be placed on each screen..

### /STRENGTHENED

Finally, in order to make the device on its own unusable, the use of an additional external media (smart card or USB token for example) to hold decryption or authentication secrets may be considered. In this case, it must be kept separate.

ANSSI-CDSE, *Passeport de conseils aux voyageurs* (Travel advice booklet), good practice,  
January 2010

# 31

## Encrypt sensitive data, in particular on hardware that can potentially be lost

### /STANDARD

Frequent journeys in a professional context and the miniaturisation of IT hardware often lead to their loss or theft in a public space. This may put the sensitive data of the organization which is stored on it at risk.

Therefore, on all mobile hardware (laptops, smartphones, USB keys, external hard drives, etc.), only data that has already been encrypted must be stored, in order to maintain its confidentiality. Only confidential information (password, smart card, PIN code, etc.) will allow the person who has it to access this data.

A partition, archive or file encryption solution may be considered depending on the needs. Here, once again, it is essential to ensure the uniqueness and robustness of the decryption method used.

As far as possible, it is advisable to start by a complete disk encryption before considering archive and file encryption. These last two respond to different needs and can potentially leave the data storage medium unencrypted (backup files from office suites for example).

Catalogue of products and qualified service providers

# 32

## Secure the network connection of devices used in a mobile working situation

### /STANDARD

In a mobile working situation, it is not uncommon for a user to need to connect to the organization's information system. Consequently, it is important to ensure this network connection is secure through the Internet. Even if the option of establishing VPN SSL/TLS tunnels is now common, the establishment of a VPN IPsec tunnel between the mobile workstation and a VPN IPsec gateway, provided by the organization, is strongly recommended.

To guarantee an optimal level of security, this VPN IPsec tunnel must be automatically established and not removable by the user, in other words no flow must be able to be sent outside of this tunnel.

For specific authentication needs on captive portals, the organization may choose to depart from automatic connection by authorising a connection upon request, or keep this recommendation by encouraging the user to use tethering on a trusted mobile phone..

### /STRENGTHENED

In order to avoid any reuse of authenticators from a stolen or lost device (saved username and password for example), it is preferable to use two-factor authentication, with a password and a certificate stored on an external medium (smart card or USB token) or a one-time password mechanism, for example.

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau* (Security recommendations relating to IPsec for the protection of network flows), technical note, August 2015

# 33

## Adopt security policies dedicated to mobile devices

### /STANDARD

Smartphones and tablets are a part of our daily personal and professional lives. The first recommendation consists precisely of not sharing personal and professional uses on the single and same device, for example by not simultaneously synchronising professional and personal email, social networks and calendar accounts, etc.

The devices, provided by the organization and used in a professional context, must be subject to a separate securing, as soon as they are connected to the organization's information system or as soon as they contain potentially sensitive professional information (mails, shared files, contacts, etc.). Consequently, the use of a centralised management solution for mobile devices is to be favoured. It will be desirable to uniformly configure the inherent security policies: a method for unlocking the device, limiting the use of the application store to validated applications from a security point of view, etc.

Otherwise, configuration prior to distribution of the device and an awareness raising session with users is desirable.

### /STRENGTHENED

Among other potentially risks, using a built-in voice assistant markedly increases the terminal's vulnerabilities to hacking and incidents of hacks have been demonstrated. For these reasons, it is therefore not advisable.

ANSSI, *Recommandations de sécurité relatives aux ordiphones* (Security recommendations relating to smartphones), technical note, July 2015

**VIII**

**KEEP THE INFORMATION SYSTEM UP TO DATE**

# 34

## Define an update policy for the components of the information system

### /STANDARD

New flaws are regularly discovered at the heart of systems and software. These are generally access doors that a hacker can exploit for a successful intrusion into the information system. It is, therefore, vital to stay informed of new vulnerabilities (follow CERT- FR alerts) and to apply the corrective security actions over all of the components of the system within the month following their publication. An update policy must therefore be defined and be a part of operational procedures.

These must specify:

- > the way in which the inventory of the information system components is carried out;
- > the sources of information relating to the publication of updates;
- > the tools to deploy the corrective actions over the stock (for examples WSUS for updates for Microsoft components, free or paid tools for third party components and other operating systems);
- > the possible qualification of corrective measure and their gradual deployment over the stock.

The obsolete components which are no longer supported by their manufacturers must be isolated from the rest of the system. This recommendation applies as much on the network level, by strict filtering of flows, as it does as regards the authentication secrets which must be dedicated to these systems.

CERT-FR: within COSSI (Information Security System Operational Centre), the governmental centre for monitoring, alerts and the response to cyberattacks (CERT-FR) ensures the French government's CERT (Computer Emergency Response Team) role. To this end, among its main missions is a technological monitoring action informing everyone on the latest developments of systems and software.



# 35

## Anticipate the software and system end of life/maintenance and limit software reliance

### /STANDARD

The use of an obsolete system or software package significantly increases the possibilities of a cyberattack. Systems become vulnerable when corrective measures are no longer proposed. Malicious tools exploiting these vulnerabilities can be spread quickly online while the publisher is not offering a security corrective measure.

To anticipate obsolescence, a certain number of precautions exist:

- > establish an inventory of the information system applications and systems and keep it up to date;
- > choose solutions with support that is ensured for a time period corresponding to their use;
- > ensure monitoring of updates and end of support dates for software;
- > keep an homogeneous software stock (the co-existence of different versions of the same product increases the risks and makes monitoring more complicated);
- > reduce software reliance, in other words, dependency on the operating of a software package compared to another, in particular when its support comes to an end;
- > include in contracts with service providers and suppliers clauses guaranteeing the monitoring of corrective security measures and the management of obsolescence;
- > identify the time periods and resources necessary (material, human, budgetary) for the migration of each software package at the end of its life (non-regression tests, backup procedure, data migration procedure, etc.).

**IX**

**SUPERVISE, AUDIT, REACT**

# 36

## Activate and configure the most important component logs

### /STANDARD

Having relevant logs is required in order to be able to detect possible malfunctions and illegal access attempts to the components of the information system.

The first stage consists of determining what the critical components of the information system are. These may be network and security devices, critical servers, sensitive user workstations, etc.

For each of these, it is advisable to analyse the configuration of logged elements (format, frequency of file rotation, maximum size of log files, event categories recorded, etc.) and to adapt it as a consequence. The critical events for security must be logged and saved for at least one year (or more, depending on the legal requirements of the business area).

A contextual assessment of the information system must be carried out and the following elements must be logged:

- > firewall: packets blocked;
- > systems and applications: authentications and authorisations (failures and successes), unplanned downtime;
- > services: protocol errors (for example the errors 403, 404 and 500 for HTTP services), traceability of flows applicable to interconnections (URL on a HTTP relay, headers of messages on a SMTP relay, etc).

In order to be able to correlate the events between the different components, their time synchronisation source (thanks to NTP protocol) must be identical.

---

**/STRENGTHENED**

If all the previous actions have been implemented, a centralisation of the logs through a dedicated measure will be able to be considered. This makes the automatic searching for suspect events easier, and allows for the archiving of logs over the long term, as well as stopping a hacker from deleting possible traces of their intrusion on the devices that he or she has compromised.

ANSSI, *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*  
(Security recommendation for the implementation of a logging system),  
technical note, December 2013

# 37

## Define and apply a backup policy for critical components

### /STANDARD

Following an exploitation incident or in the context of managing an intrusion, the availability of backups, saved in a safe place, is essential to continue the activity. Formalising a regularly updated backup policy is therefore highly recommended. This aims to define the requirements in terms of backing up information, software and systems.

This policy must, at least, integrate the following elements:

- > the list of data judged vital for the organization and the servers concerned;
- > the different types of backup (for example the offline mode);
- > the frequency of backups;
- > the administration and backup execution procedure;
- > the storage information and the access restrictions to backups;
- > the testing and restoration procedures;
- > the destruction of media that contained backups.

The restoration tests may be carried out in several ways:

- > systematic, through a task scheduler for important applications;
- > one-off, in the event of an error in files;
- > general, for complete backup and restoration of the information system.

### /STRENGTHENED

Once this backup policy has been established, it is desirable to plan, at least once per year, a data restoration exercise and to keep a technical log of the results.

# 38

## Undertake regular controls and security audits then apply the associated corrective actions

### /STRENGTHENED

Carrying out regular audits (at least once per year) of the information system is essential as this makes it possible to correctly assess the effectiveness of measures implemented and their maintenance over time. These controls and audits are also able to measure the gaps that may remain between the theory and the practice.

They can be carried out by possible internal audit teams or by specialised external companies. Depending on the scope to test, technical and/or organisational audits will be carried out by the professionals called upon. These audits are especially necessary as the organization must comply with the regulations and legal obligations directly linked to its activities.

Following these audits, corrective actions must be identified, their application planned and monitoring points organised at regular intervals. For higher efficiency, indicators on the state of progress of the action plan may be integrated into the overview for the management.

Although security audits participate in the security of the information system by being able to show possible vulnerabilities, they are never proof of their absence and therefore do not negate the need for other control measures.

The information system security audit service providers (PASSI) qualified by ANSSI deliver architecture audit, configuration, source code, intrusion test and organisational and physical audit services.

# 39

## Designate a point of contact in information system security and make sure staff are aware of him or her

### /STANDARD

All organizations must have a point of contact in information system security who will be supported by the management or an executive committee, depending on the maturity level of the organisation.

This point of contact must be known to all the users and will be the first person to call for all questions relating to information system security:

- > defining the rules to apply according to the context;
- > verifying the application of rules;
- > raising users' awareness and defining a training plan for IT stakeholders;
- > centralising and dealing with security incidents noticed or raised by users.

This point of contact must be trained in information system security and crisis management.

In larger organizations, this correspondent can be designated to become the CISO representative. He or she may, for example, raise users' grievances and identify the themes to deal with in the context of awareness raising, therefore allowing the security level of the information system to be raised within the organization.

# 40

## Define a security incident management procedure

### /STANDARD

Noticing unusual behaviour from a workstation or a server (impossible connection, significant activity, unusual activity, unauthorised open services, files created, modified or deleted without authorisation, multiple anti-virus warnings, etc.) may be a warning of a possible intrusion.

A bad reaction in the event of a security incident can make the situation worse and prevent the problem from being dealt properly. The right reaction is to disconnect the device from the network, to stop the attack. However, you must keep it powered and not restart it, so as to not lose useful information for analysing the attack. You must then alert the management, as well as the information system security point of contact.

He or she may get in contact with the security incident response service providers (PRIS) in order to carry out the necessary technical operations (physically copying the disk, analysing the memory, logs and possible malware, etc.) and determine if other elements of the information system have been compromised. This will also concern coming up with a response to provide, in order to remove possible malware and the access that the hacker may have and to change compromised passwords. Any incident must be recorded in a centralised register. Charges may also be pressed with the competent legal service.

The security incident response service providers (PRIS) get involved when signals match up, leading to malicious computing activity being suspected or proven within an information system. As these services are critical to the sustainability of information systems, ANSSI has created a reference document, the aim of which is to provide those ordering such services the necessary guarantees vis-a-vis these service providers, both in terms of competency and trust.



**X**

**TO GO EVEN FURTHER**

## 41

Carry out a formal  
risk assessment**/STRENGTHENED**

Each organization develops within a complex computing environment specific to itself. As such, any position taken or action plan involving the information system security must be considered in light of the risks foreseen by the management. Whether it is organisational or technical measures, their implementation represents a cost for the organization, which needs to ensure that they are able to reduce an identified risk to an acceptable level.

In the most sensitive cases, the risk analysis may call into question certain previous choices. This may be the case if the probability of an event appearing and its potential consequences prove critical for the organization and there is no preventive action to control it.

The recommended approach consists, in broad terms, of defining the context, assessing the risks and dealing with them. The risk assessment generally works by considering two areas: the likelihood and the impacts. This is then followed by the creation of a risk treatment plan to be validated by a designated authority at a higher level.

Three kinds of approach can be considered to control the risks associated with the information system:

- > the recourse to best IT security practices;
- > a systematic risk analysis based on feedback from users;
- > a structured risk management formalised by a dedicated methodology.

---

In this last case, the EBIOS method referenced by ANSSI is recommended. It is able to write down security needs, identify the security objectives and determine the security demands

The EBIOS (Expression of Needs and Identification of Security Objectives) risk analysis method is able to assess and deal with the risks relating to information system security. It is also able to communicate on this issue within the organization and towards its partners, therefore constituting a comprehensive information system security risk management tool.

## 42

## Favour the use of products and services qualified by ANSSI

**/STRENGTHENED**

The qualification delivered by ANSSI offers security and trust guarantees to purchasers of solutions listed in the product catalogues and qualified service providers that the agency publishes.

Beyond organizations subject to regulation, more generally ANSSI encourages all companies and French administrations to use products that it qualifies; the only proof of a serious and in depth study of the technical functioning of the solution and its ecosystem.

In terms of qualified service providers, this certification is able to respond to the cybersecurity stakes and projects for the entirety of the French companies that ANSSI could not address on its own. Assessed on technical and organisational criteria, the qualified service providers cover the vast majority of the information system security jobs. Therefore, depending on its needs and the geographical position an organization will be able to call on an Information System Security Audit Service Provider (PASSI), a Security Incident Response Service Provider (PRIS), a Security Incident Detection Service Provider (PDIS) or a Cloud Computing Service Provider (SecNumCloud)

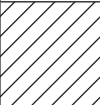
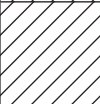
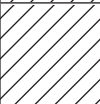
.

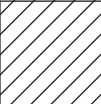


## MONITORING TOOL

I - Raise awareness and train		STANDARD	STRENGTHENED
1	Train the operational teams in information system security		
2	Raise users' awareness about basic information security		
3	Control outsourced services		

II - Know the information system		STANDARD	STRENGTHENED
4	Identify the most sensitive information and servers and keep a network diagram		
5	Have an exhaustive inventory of privileged accounts and keep it updated		
6	Organise the procedures relating to users joining, departing and changing positions		
7	Only allow controlled devices to connect to the network of the organization		

III - Authenticate and control accesses		STANDARD	STRENGTHENED
8	Identify each individual accessing the system by name and distinguish the user/administrator roles		
9	Allocate the correct rights to the information system's sensitive resources		
10	Set and verify rules for the choice and size of passwords		
11	Protect passwords stored on systems		
12	Change the default authentication settings on devices and services		
13	Prefer a two-factor authentication when possible		

IV - Secure the devices		STANDARD	STRENGTHENED
14	Implement a minimum level of security across the whole IT stock		
15	Protect against threats relating to the use of removable media		
16	Use a centralised management tool to standardise security policies		


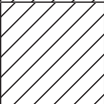
17	Activate and configure the firewall on workstations		
18	Encrypt sensitive data sent through the Internet		



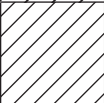
V - Secure the network		STANDARD	STRENGTHENED
19	Segment the network and implement a partitioning between these areas		
20	Ensure the security of Wi-Fi access networks and that users are separated		
21	Use secure network protocols when they exist		
22	Implement a secure access gateway to the Internet		
23	Segregate the services visible from the Internet from the rest of the information system		
24	Protect your professional email		
25	Secure the dedicated network interconnections with partners		
26	Control and protect access to the server rooms and technical areas		



<b>VI - Secure administration</b>		STANDARD	STRENGTHENED
27	Prohibit Internet access from devices or servers used by the information system administration		
28	Use a dedicated and separated network for information system administration		
29	Reduce administration rights on workstations to strictly operational needs		

<b>VII - Manage mobile working</b>		STANDARD	STRENGTHENED
30	Take measures to physically secure mobile devices		
31	Encrypt sensitive data , in particular on hardware that can potentially be lost		
32	Secure the network connection of devices used in a mobile working situation		
33	Adopt security policies dedicated to mobile devices		

<b>VIII - Keep the information system up to date</b>		STANDARD	STRENGTHENED
34	Define an update policy for the components of the information system		
35	Anticipate the software and system end of life/ maintenance and limit software reliance		

<b>IX - Supervise, audit, react</b>		STANDARD	STRENGTHENED
36	Activate and configure the most important component logs		
37	Define and apply a backup policy for critical components		
38	Undertake regular controls and security audits then apply the associated corrective actions		
39	Designate a point of contact in information system security and make sure staff are aware of him or her		
40	Define a security incident management procedure		

X - To go even further		STANDARD	STRENGTHENED
<b>41</b>	Carry out a formal risk assessment		
<b>42</b>	Favour the use of products and services qualified by ANSSI		

## BIBLIOGRAPHY

### Guides and methods

ANSSI, *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine* (IT and digital tools user charter), guide, June 2017  
[www.ssi.gouv.fr/guide-bonnes-pratiques/](http://www.ssi.gouv.fr/guide-bonnes-pratiques/)

ANSSI, *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)* (Best practice for acquiring and using domain names), guide, February 2010  
[www.ssi.gouv.fr/ebios/](http://www.ssi.gouv.fr/ebios/)

ANSSI, *Guide de l'externalisation – Maîtriser les risques de l'infogérance* (Outsourcing guide - Controlling the risks of managed services), guide, January 2010  
[www.ssi.gouv.fr/externalisation/](http://www.ssi.gouv.fr/externalisation/)  
[www.ssi.gouv.fr/infogérance/](http://www.ssi.gouv.fr/infogérance/)

ANSSI-CDSE, *Passeport de conseils aux voyageurs*, (Controlling the risks of managed services), guide, December 2010  
[www.ssi.gouv.fr/passeport-de-conseils-aux-voyageurs/](http://www.ssi.gouv.fr/passeport-de-conseils-aux-voyageurs/)

### Technical notes

ANSSI, *Guide de définition d'une architecture de passerelle d'interconnexion sécurisée* (Definition guide for secure gateway interconnection architecture), technical note, December 2011  
[www.ssi.gouv.fr/passerelle-interconnexion/](http://www.ssi.gouv.fr/passerelle-interconnexion/)

ANSSI, *Recommandations de sécurité relatives aux mots de passe* (Security recommendations relating to passwords), technical note, June 2012  
[www.ssi.gouv.fr/mots-de-passe/](http://www.ssi.gouv.fr/mots-de-passe/)

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu* (Recommendations for defining a network filtering policy for a firewall), technical note, March 2013  
[www.ssi.gouv.fr/politique-filtrage-parefeu/](http://www.ssi.gouv.fr/politique-filtrage-parefeu/)

ANSSI, *Recommandations de sécurité relatives aux réseaux Wi-Fi* (Security recommendations relating to Wi-Fi networks), technical note, September 2013  
[www.ssi.gouv.fr/nt-wifi/](http://www.ssi.gouv.fr/nt-wifi/)

ANSSI, *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows* (Recommendations for the implementation of a software restriction policy in Windows), technical note, December 2013  
[www.ssi.gouv.fr/windows-restrictions-logicielles/](http://www.ssi.gouv.fr/windows-restrictions-logicielles/)

ANSSI, *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation* (Security recommendations for the implementation of a logging system), technical note, December 2013  
[www.ssi.gouv.fr/journalisation/](http://www.ssi.gouv.fr/journalisation/)

ANSSI, *Recommandations de sécurité relatives à Active Directory* (Security recommendations relating to Active Directory), technical note, September 2014  
[www.ssi.gouv.fr/Active-Directory/](http://www.ssi.gouv.fr/Active-Directory/)

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information* (Recommendations relating to the secure administration of information systems), technical note, February 2015  
[www.ssi.gouv.fr/securisation-admin-si/](http://www.ssi.gouv.fr/securisation-admin-si/)

ANSSI, *Recommandations de sécurité relatives aux ordiphones* (Security recommendations relating to smartphones), technical note, July 2015  
[www.ssi.gouv.fr/securisation-ordiphones/](http://www.ssi.gouv.fr/securisation-ordiphones/)

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau* (Recommendations for securing networks with IPsec), technical note, August 2015

[www.ssi.gouv.fr/ipsec/](http://www.ssi.gouv.fr/ipsec/)

ANSSI, *Recommandations de configuration d'un système GNU/Linux* (Configuration recommendations for a GNU/Linux system), technical note, January 2016

[www.ssi.gouv.fr/reco-securite-systeme-linux/](http://www.ssi.gouv.fr/reco-securite-systeme-linux/)

## Online resources

ANSSI's website

Catalogue of products and qualified service providers

[www.ssi.gouv.fr/qualifications/](http://www.ssi.gouv.fr/qualifications/)

Twitter

@ANSSI\_FR

[www.twitter.com/anssi\\_fr](http://www.twitter.com/anssi_fr)

CERT-FR

[www.cert.ssi.gouv.fr](http://www.cert.ssi.gouv.fr)

CNIL

[www.cnil.fr](http://www.cnil.fr)

## References

Douglas Adams, *The Hitchhiker's Guide to the Galaxy* (or H2G2), science fiction novel, 1979



Version 2.0 - September 2017

20170928-1106

---

Licence Ouverte/Open Licence (Etalab - V1)

---

**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

[www.ssi.gov.fr](http://www.ssi.gov.fr) / [communication@ssi.gov.fr](mailto:communication@ssi.gov.fr)



Premier ministre

