INTER-MINISTERIAL

DIRECTIVE PERTAINING TO THE PROTECTION OF SENSITIVE INFORMATION SYSTEMS

No. 901/SGDSN/ANSSI

NOR: PRMD1503279J

Table of contents

Section I - Definition and Scope 4
Article 1: Definitions 4
Article 2: Scope of application 4
Article 3: Strategic principles 5
Article 4: Application of the regulations 5
Section II - Protection of sensitive information systems 6
Article 5: Determination of the sensitivity of information 6
Article 6: Governance of the protection of information systems 6
Article 7: Risk control 6
Article 8: Accreditation of sensitive information systems 6
Article 9: Protection of information systems 7
Article 10: Handling of information systems security incidents 7
Article 11: Evaluation of security level 7
Article 12: Relations with State authorities 7
Section III - Protection of *Diffusion Restreinte* information systems 8
Article 13: Accreditation of *Diffusion Restreinte* information systems 8
Article 14: Processing information marked as *Diffusion Restreinte* 8
Article 15: Physical protection of premises 8
Article 16: Outsourcing 8
Article 17: Use in an uncontrolled environment 9
Article 18: Audio-visual media 9
Article 19: Authorisation of derogations 9
Section IV - Transitional and final provisions 10
Article 20: Transitional provisions 10
Article 21: Repeal 10
Appendix 1 - Regulations for entities outside the scope of application of the PSSIE 11
Appendix 2 - Different classes of network 38
Appendix 3 - Reference documents 39

This directive defines the objectives and regulations pertaining to the protection of sensitive information systems, particularly those which process information marked as *Diffusion Restreinte* (Restricted distribution).

This directive is addressed to all physical or legal persons involved with these systems.

Observance of the regulations contributes towards ensuring continuity of the activities of the entity which implements the information system, protecting this entity's image, preventing compromise of sensitive information and ensuring the security of persons and property.

These regulations may be specified on a case-by-case basis drawing on existing technical norms and the technical guidance documents and recommendations of the french national information security agency (ANSSI).

Section I - Definition and Scope

Article 1: Definitions

Sensitive information systems are those which process information whose disclosure to non-authorised persons, and whose modification or non-availability prejudices the achievement of the objectives of the entities which implement them.

Diffusion Restreinte **information systems** are **sensitive information systems** which process information marked as *Diffusion Restreinte*[1] or the European or international equivalents.

Article 2: Scope of application

2.1 The directive applies:

- to State administrative services[2] which implement **sensitive information systems**;
- public or private entities subject to the regulation pertaining to the protection of the Nation's scientific and technological potential (PPST)[3] and which implement **sensitive information systems**[4]**;**
- to all other public or private entities which implement ***Diffusion Restreinte*** **information systems**.

2.2 This directive has recommendatory value for all other public or private entities which implement **sensitive information systems,** particularly systems processing information governed by specific security obligations[5].

2.3 This directive does not apply to information systems processing information covered by national defence secrecy[6].

[1] See article 5 and appendix 3, entitled "Regulations for the protection of information or media marked as *" Diffusion Restreinte "***,** of General Inter-Ministerial Directive No. 1300/SGDSN/PSE/PSD of 30 November 2011 on the protection of national defence secrecy. The wording *Diffusion Restreinte* does not represent a classification level but is a protective term alerting the user to the discretion that must be exercised when handling the information to which this wording is applied.

[2] The State administrative services as defined in this directive are the Central Administrative Services, the National Public Bodies, devolved State Services and Independent Administrative Authorities.

[3] The legislative framework of the PPST is defined in article R. 413-5-1 of the French penal code and by Decree No. 2011-1425 of 2 November 2011 in application of article 413-7 of the penal code and pertaining to the protection of the Nation's scientific and technological potential and by the order of 3 July 2012 pertaining to the protection of the Nation's scientific and technological potential.

[4] Except where they process classified information and are in consequence governed by texts pertaining to the protection of information covered by national defence secrecy, information systems which are implemented by an entity subject to the regulations pertaining to PPST and which process information pertaining to specialisms with expertise that is capable of being misappropriated for terrorist ends or for the proliferation of arms of mass destruction and their vectors constitute *Diffusion Restreinte* information systems.

[5] This particularly concerns systems processing information covered by professional secrecy, constituting correspondence that is private or mentioned in article 6 of the law No. 78-753 of 17 July 1978 establishing various measures to improve relations between the administrative services and the public and various administrative, social and fiscal provisions. This also concerns the information systems mentioned in the Ordinance No. 2005-1516 of 8 December 2005 pertaining to electronic exchanges between users and the administrative authorities and between administrative authorities.

[6] These systems are governed by articles R. 2311-1 et seq of the Defence Code and by the General Inter-Ministerial Directive No. 1300/SGDSN/PSE/PSD of 30 November 2011 on the protection of national defence secrecy, notably its Section V.

Article 3: Strategic principles

The regulations described in this directive are based on five strategic principles:

- to set up an organisation dedicated to the security of information systems, including preventive and defensive components and based on identified human, material and financial resources;
- to regularly conduct risk assessments, adopting a continuous improvement process of the security of each system during its lifetime;
- to defend in depth, by ensuring in the design stage that if one of the security measures is compromised or faulty, others will ensure the protection of sensitive information;
- to observe the fundamental rules of computer hygiene, defined by ANSSI, implemented by information systems administrators trained for this purpose;
- to use security products that are approved, qualified, or failing that, certified and to use trustworthy service providers certified by ANSSI.

Article 4: Application of the regulations

4.1 Application of the regulations to **sensitive information systems**

The State administrative services which implement **sensitive information systems** apply the State Information Systems Security Policy (PSSIE)[7]. A State administrative service which observes the PSSIE is considered to comply with all the provisions of Section II.

The public and private entities mentioned in article 2.1 which implement **sensitive information systems** apply the regulations provided in Section II and those provided in appendix 1. These latter are the PSSIE regulations adapted to entities located outside the scope of application of this security policy.

4.2 Application of the regulations to ***Diffusion Restreinte*** **information systems**

The State administrative services which implement ***Diffusion Restreinte*** **information systems** apply the PSSIE and the regulations provided for in Section III.

The public or private bodies which implement ***Diffusion Restreinte*** **information systems** apply the regulations provided for in Sections II and III and appendix 1.

[7] The PSSIE was approved by a circular from the Prime Minister signed 17 July 2014.

Section II - Protection of sensitive information systems

Article 5: Determination of the sensitivity of information

Each entity implementing **a sensitive information system**:

- identifies the sensitive information that it processes;
- marks this information using means that it selects;
- determines, if necessary, a sensitivity scale corresponding to levels bearing on the availability, integrity and confidentiality of the information in its sensitive information system;
- applies appropriate protective measures.

When sensitive information transits between several entities, its sensitivity level is explicitly mentioned by the issuing entity so that in consequence it is protected by the receiving entity in terms of availability, integrity and confidentiality, during and after its transit.

Article 6: Governance of the protection of information systems

Each entity:

- applies an information systems security policy (PSSI), validated at the highest level of the entity and covering all aspects, technical and other, of security (communication, human and financial resources, legal aspects, *etc.)*;
- organises governance and allocates responsibilities regarding information systems security.

Article 7: Risk control

The PSSI of the entity results from a risk assessment performed:

- for all risks, not just technical risks, whether they are human in origin or not;
- for each of the entity's information systems;
- appreciating the impact that a threat to a system component could have on the entity's operations, its image, its assets and the security of persons and property.

Article 8: Accreditation of sensitive information systems

All **sensitive information systems** must be subject to security accreditation before being commissioned. Particular mention is made in the accreditation dossier of the residual risks, that is those which are not covered by protective measures.

The accreditation authority must be chosen from within the entity, at a sufficiently high hierarchical level to assume the responsibility pertaining to the decision on accreditation. It accepts the residual risks in particular. In principle it is the authority that employs the system.

In giving accreditation, the accreditation authority declares that the information system complies with the regulations provided for in this directive.

Article 9: Protection of information systems

The entity has a map of all information systems for which it is responsible. This map is kept up to date. It is needed by the entity to ensure the protection of its information system.

The entity protects its information system against the threats identified throughout its lifetime. Protection is based on several components:

- physical: it delays or prevents physical access by non-authorised persons to the premises, to systems and to information, while maintaining access availability for authorised persons. It also enables the avoidance and detection of physical incidents such as faulty power supply, faulty air conditioning, fire and water damage;
- logical: it enables protection against malicious and accidental cyberattacks but it particularly facilitates protection of networks, equipment, data and their media, logical access and systems administration;
- organisational: it is implemented in accordance with the processes explicitly defined in the entity's PSSI.

In the event of a raised level of threat, the entity strengthens vigilance and protection measures for its systems.

Article 10: Handling of information systems security incidents

Even though protected, the entity prepares itself for attacks on its information system. It integrates information systems security (SSI) into its crisis management procedures and its periodic exercises. To be able to act to reduce the impact of attacks and incidents, it acquires:

- a capacity to detect, analyse, characterize and respond, in particular to ensure the continuity of its operations;
- an incident management process in order to detect and analyse the attacks and to respond to unusual events.

Experience feedback on the handling of incidents is expected after every event.

Article 11: Evaluation of security level

The entity continuously evaluates the security level of its information system and the residual risks. It carries out checks on a regular basis and conducts operational and technical security audits of its information system. This evaluation enables the impact of attacks and incidents to be reduced and the continuity of service of the entity to be ensured.

Article 12: Relations with State authorities

Without prejudice to the special legislative and regulatory provisions, particularly those applicable to operators of vital importance, each entity cooperates with State authorities such as ANSSI or their line ministries to ensure the security of its information system. In the event of a crisis, it responds to the requests of these authorities.

Section III - Protection of *Diffusion Restreinte* information systems

Article 13: Accreditation of *Diffusion Restreinte* information systems

All *Diffusion Restreinte* information systems are accredited in this regard under the conditions provided for in article 8. In particular, the accreditation anticipates the way in which the destruction of the system itself or of other media which have contained information marked as *Diffusion Restreinte* is controlled and managed.

Article 14: Processing information marked as *Diffusion Restreinte*

Depending on its need and its technical, human and financial resources, the entity chooses, in compliance with the provisions of this article and appendix 2, the network class on which information marked as *Diffusion Restreinte* is processed.

The processing of unencrypted information marked as *Diffusion Restreinte* in particular its storage and distribution, is carried out on class 1 or class 2 networks.

It is strongly recommended that a class 2 network is chosen. In effect, any connection to a public network represents in itself a vulnerability which can easily lead to the compromise of information.

Information marked as *Diffusion Restreinte* is encrypted using means authorised at this level by ANSSI when it is in transit or is stored outside an area that is physically protected under the conditions provided for in article 15.

Article 15: Physical protection of premises

Physical security measures are chosen that are proportionate to the threats determined by the risk assessment provided for in article 7. They aim both to prevent the loss, modification or deterioration of information marked as *Diffusion Restreinte* and to collect information to resolve computer incidents by:

- defending the boundaries of the area to be protected with a physical perimeter barrier;
- discouraging non-authorised access by all appropriate physical measures;
- controlling access to the premises using electronic, electromechanical and human resources;
- preserving access traceability;
- protecting against intrusions with a detection system (this system may replace a perimeter barrier or supplement it to strengthen the level of security).

Article 16: Outsourcing

In the event that a service which implements a *Diffusion Restreinte* information system is outsourced, the entity and its service provider take account of the recommendations mentioned in the ANSSI guidance documents relating to outsourcing[8]. Their contract guarantees the compliance of the information system with the regulations provided for in this directive. As far as possible, the service will be carried out on national territory.

[8] ANSSI Guidance Document "Controlling risks associated with managed services - Outsourcing information systems", http//www.ssi.gouv.ff/infogerance.

All entities are recommended to choose trustworthy service providers certified by ANSSI.

Article 17: Use in an uncontrolled environment

Information marked as *Diffusion Restreinte* contained in nomad devices (laptops, removable media, phones, *etc.)* is encrypted using means authorised by ANSSI, in order to limit the risk of disclosure in the event of loss or theft.

Specific precautions are taken when consulting electronic documents marked as *Diffusion Restreinte* in public places (use of a screen privacy filter, continuous monitoring of the nomad workstation itself, of the surrounding areas, of media marked as *Diffusion Restreinte* and of the equipment that is using it).

The connection of personal equipment to a *Diffusion Restreinte* information system is prohibited.

The same applies to the connection of nomad equipment processing information marked as *Diffusion Restreinte* to any information system other than those approved by the entity to process such information, unless the accreditation of the information system to which the nomad device belongs allows this and if the regulations provided for in this directive are observed.

Article 18: Audio-visual media

Before circulating information marked as *Diffusion Restreinte* on audiovisual media, the person in charge of broadcasting shall check that participants need to know this information. He/she shall also ensure that the information systems used are approved to process information marked as *Diffusion Restreinte*.

On this occasion, particular attention shall be paid to the potential photographic, video or audio capture of information. If needed, such capture is forbidden.

Article 19: Authorisation of derogations

When circumstances require, time-limited derogations from the regulations provided for in this directive may be granted to an entity for a *Restricted Distribution* system that it implements. Derogations are granted by the Senior Defence and Security Official (HFDS) from the ministry with responsibility for the entity which implements the information system. ANSSI is informed of derogation authorisations and their justification.

Section IV - Transitional and final provisions

Article 20: Transitional provisions

Entities have a three-year period from the publication date of this directive to render their *Diffusion Restreinte* information systems, commissioned before the publication date of this directive, or during the six months after this date, compliant with the regulations it stipulates. During this period, entities draw up a list of shortcomings relating to the regulations provided for in this directive, and make the list available to ANSSI.

Article 21: Repeal

This directive repeals recommendation No. 901/DISSI/SCSSI of the 2 March 1994 on the protection of information systems processing sensitive defence information which is non classified and recommendation No. 600/DISSI/SCSSI of March 1993 on the protection of sensitive information not covered by defence secrecy.

Paris, 28 January 2015

Guillaume POUPARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

Appendix 1 - Regulations for entities outside the scope of application of the PSSIE[9]

Policy, organisation, governance

Objective 1:

To set up an appropriate organisation, guaranteeing the preventive and responsive application of security.

SSI Organisation

ORG-SSI: SSI organisation. A structure dedicated to SSI (Information Systems Security) is deployed in each entity. This organisation defines the responsibilities relating to internal staff and third parties, modalities for coordination with the external authorities and the modalities for applying protective measures. Procedures for the application of protective measures are written down and everyone is informed of them.

SSI Personnel

ORG-ACT-SSI: identification of SSI personnel. The SSI structure is based on clearly identified personnel, responsible for the general implementation of the PSSI.

Internal responsibilities

ORG-RSSI: appointment of the SSI Supervisor. The entity's management relies on one or more Information Systems Security Supervisors (RSSI), responsible for assisting it with SSI direction and management. Local SSI officers may be appointed as needed, to provide a representative for the RSSI. The entity's RSSI has the measures for applying the PSSI validated by management and oversees their application. Alternative names for the roles mentioned above may be used if necessary.

ORG-RESP: formalisation of responsibilities. An organisation memorandum establishes the division of responsibilities with respect to SSI within each entity and at local level. On most occasions, this memorandum will be put forward by the RSSI and validated by the entity's management.

Responsibilities towards third parties

ORG-TIERS: contractual management of third parties. The RSSI coordinates actions enabling the incorporation of clauses related to SSI in all contracts or agreements involving third party access to information or to computing resources.

PSSI

QRG-P1L-PSSI: definition and direction of PSSI. Each entity establishes a PSSI, validated by management. A process control structure is defined for the PSSI. This structure is responsible for setting up the PSSI, its development, monitoring and control.

[9] These regulations are adapted from the State information systems security policy.

Application of security measures within the entity

ORG-APP-INSTR: application of the directive within the entity. The RSSI plans PSSI implementation. He reports regularly to the entity's management on the application of security measures.

QRG-APP-DOCS: formalisation of application documents. The RSSI creates and updates the documents, approved by the entity's management, enabling the application of PSSI measures.

Human resources

Objective 2:

To make people the key asset of information systems.

Users

RH-SSI: SSI application charter. A PSSI application charter, recapitulating the practical measures for the secure use of computing resources and developed under the direction of the SSI functional chain, is communicated to all staff in each entity. This charter must be legally enforceable, and if possible, incorporated into the internal regulations of the entity. Non-permanent personnel (interns, temporary personnel, service providers) are informed of their obligations as part of their use of information systems.

Permanent personnel

RH-MOTIV: selection and sensitisation of persons holding key SSI positions. Particular attention must be paid to the recruitment of key SSI personnel: RSSI, local SSI officers and security administrators. The RSSIs and their local officers must receive specific training in SSI. Information systems administrators must be made aware of the duties of their job on a regular basis and must take care to observe these requirements in their daily activities.

RH-CONF: trusted personnel. All persons handling sensitive information must do so with particular care, observing the regulations in force. They are reminded of the possible sanctions applying to cases of negligence or malice.

RH-UTIL: awareness of information systems users. Each user must be regularly informed of the security requirements which affect him/her. He/she must be trained in the use of work tools in accordance with the SSI regulations.

Movement of personnel

RH-MOUV: management of arrivals, transfers and departures. A procedure to manage the arrivals, transfers, and departures of colleagues must be formalised and strictly applied. This procedure must at least cover:

- the management and cancellation of accounts and access rights to information systems, including for partners and external service providers;
- management of the access control system to the premises;
- management of mobile equipment;
- management of the control of individual clearances.

Non-permanent personnel

RH-NPERM: management of non-permanent personnel (interns, temporary personnel, service providers). The PSSI regulations apply to all non-permanent personnel who use an entity's information system. The pre-existing contractual provisions governing the employment of such personnel are amended if necessary. Guidance by a permanent member of staff is provided for all non-permanent personnel, in order to inform them of these regulations and to control their application.

Asset management

Objective 3:

Keeping a detailed and complete information system map updated.

GDB-INVENT: inventory of computing resources. Each entity creates an inventory of computing resources under its responsibility and keeps it updated, using suitable tools. This inventory is made available to the RSSI and ANSSI in case of a need for operational coordination. It includes the list of hardware and software components used and their exact versions. It comprises a configuration database, kept updated and made available to the RSSI.

The allocations history of the inventoried items must be kept in accordance with the regulations in force.

GDB-CARTO: mapping. The map gives details of the computer centres, the network architectures, with identification of sensitive points and the sensitivity of information handled, and describes the security level expected. This map is kept updated and made available to the RSSI and ANSSI in case of a need for operational coordination.

Objective 4:

To classify information so as to adapt protective measures.

GDB-QUALIF-SENSI: classification of information. The sensitivity of all information must be assessed. The systematic marking of documents, in accordance with sensitivity level, is highly recommended.

GDB-PROT-IS: protection of information. User must protect the information which he handle as part of his job, in accordance with its sensitivity and throughout its life cycle, from its creation to its potential destruction.

Integration of the SSI in the information systems life cycle

Objective 5:

To appraise, handle, and communicate the risks relating to information systems security.

Risk management and security accreditation

INT-HOMOLOG-SSI: accreditation of information systems security. Each information system must be subject to an accreditation decision regarding its security before being commissioned. The accreditation is the act according to which an authority, referred to as the accreditation authority, appointed by the entity's management, formally confirms to users that the information system is protected in compliance with the security objectives established. If need be, the accreditation decision is taken after obtaining the opinion of an accreditation committee. This decision is based on a risk assessment tailored to stakes raised by the system under consideration and specifies the conditions of use.

Objective 6:

To dynamically manage protective measures throughout the information system lifecycle.

Maintenance of information systems in a secure condition

INT-SSI: integration of security into projects. The security of information systems must be taken into account at all stages of IT projects, from the design and specification of the system until its withdrawal from service, under the control of the accreditation authority.

INT-QUOT-SSI: day-to-day implementation of SSI. The security of information systems is addressed on a day-to-day basis by the practice of computer hygiene. Maintenance of a system in a secure condition during the design, development and withdrawal phases is defined in written procedures.

NT-TDB: create an SSI dashboard. An SSI dashboard is set up and kept updated. It will provide the RSSI and the authorities with a general view of the level of security and of its progress, thus making direction of the SSI more efficient. At strategic level, the SSI dashboard enables the application of the security policy to be monitored, and allows elements appropriate to the qualification of resources before their allocation to SSI to be made available. In terms of process management, the setting up of this dashboard enables control of

the achievement of operational objectives, improvement of service quality, and the earliest detection of delays in achieving certain security objectives.

Objective 7:

To use products and services whose security has been evaluated and certified in accordance with procedures recognised by ANSSI, in order to strengthen information systems protection.

Labelled security products and services

INT-AQ-PSL: acquisition of trusted security products and services. When available, trusted security products and services labelled (approved, qualified or certified) by ANSSI must be used.

Objective 8:

To ensure that security requirements are met when services provided by a third party are used.

Management of service providers

INT-PRES-CS: security clauses. All service provision in the information systems field occurs within the framework of security clauses. These clauses specify the SSI measures that service providers must observe in the course of their activities.

INT-PRES-CNTRL: monitoring and control of services provided. Maintenance of a security level over time requires dual control:

- one carried out regularly by the team supervising the service provision, which relates to the actions of the subcontractor and compliance with the specifications;
- the other carried out by an external team, which relates to the pertinence of the specifications upstream of projects, the conformity of the subcontractor's solutions in the acceptance phase and the overall level of security obtained in the production phase.

INT-REX-AR: risk analysis. All outsourcing operations are based on a prior risk analysis, so that the security objectives are determined and appropriate measures defined. The set of security objectives so determined enables definition of a security target that will serve as a framework for the contract established with the service provider.

INT-REX-HB: hosting. It is obligatory to host sensitive administrative data on national territory, unless there is a derogation, duly justified and detailed in the accreditation decision.

INT-REX-HS: hosting and security clauses. All hosting contracts detail the provisions implemented to take account of information systems security. These are in particular the measures taken to ensure the maintenance of systems in a secure condition and to enable effective crisis management (conditions of access to logs, establishing penalties, *etc.).*

Pysical security

Objective 9:

To involve the physical securing of information systems with the physical securing of the premises and in the associated processes.

PHY-ZONES: division of sites into security zones. The division of sites into physical security zones must be carried out, in liaison with the RSSI, the local SSI officers and the services responsible for the building, security and general resources. Precise criteria for authorising access to each security zone are established.

Security regulations applying to public reception areas

PHY-PUBL: network access in public reception areas. All access to the network installed in a public reception area must be filtered or isolated from the rest of the entity's computer network.

PHY-SENS: protection of sensitive information in reception areas. Processing sensitive information in reception areas should be avoided. If such processing is strictly necessary, it must remain a limited and exceptional event. Specific measures are then adopted, particularly regarding audiovisual protection and protection of the information stored on data carriers.

Supplementary security regulations applying to technical premises

PHY-TECH: physical security of technical rooms. Access to technical rooms housing power supply and energy distribution equipment or network and telephony equipment must be physically protected.

PHY-TELECOM: protection of electrical cables and telecommunications. Network cabling must be protected against damage and interceptions of the communications that it transmits. In addition, patch panels and cable rooms must be situated out of public reception areas and access to them must be controlled.

PHY-CTRL: anti-entrapment checks. On particularly sensitive information systems, regular anti-entrapment checks should be made, performed by trained personnel. They may call on specialised services for operations referred to as 'dust removal'.

Objective 10:

To provide physical protection of computer centres proportionate to the issues raised by the concentration of resources and data they house.

General regulations

PHY-CI-LOC: division of premises into security zones. The computer centre must be divided into physical security zones, in liaison with the RSSI and the services responsible for the building, security and general resources. Regulations must be drafted fixing the conditions of access to these different areas.

PHY-CI-HEBERG: service agreement in the case of third party hosting. In the case where all or part of the computer centre premises is managed by a third party, a service agreement, defining mutual responsibilities with respect to security, must be put in place between this third party and the entity.

Supplementary security regulations applying to internal and restricted zones

PHY-CI-CTRLACC: control of physical access. Access to internal zones (authorised solely for computer centre personnel or accompanied visitors) and restricted areas (authorised persons and accompanied visitors only) must be based on a physical access control system. This system must rely on labelled security products, when they are available, and must be rigorously maintained in a secure condition.

PHY-CI-MOYENS: delivering the means of physical access. Delivery of the means of physical access must comply with a formal process enabling verification of the identity of the person and is based on the personnel arrival and departure processes. Personnel other than that explicitly authorised or empowered but nevertheless called on to operate in the internal or restricted zones (building maintenance and repair, maintenance and repair of non IT equipment, cleaning, visitors), access these zones under permanent and systematic supervision.

PHY-CI-TRACE: access traceability. A means for tracking access by external visitors to restricted zones must be set up. These records are kept for a year, in accordance with the regulations protecting personal data.

Supplementary security regulations applying to computer rooms and technical rooms

PHY-CI-ENERGIE: energy room. The sector equipment power supply must be of the highest standard, so as to guard against compromising the safety of persons and equipment through an electrical fault.

PHY-CI-CLIM: air conditioning. An air conditioning system must be installed matching the energy requirements of the information system. Response procedures in the event of breakdown, known by staff, must be developed and verified annually. These provisions aim to prevent any overheating of equipment, which may cause a loss of service or even deterioration of equipment.

PHY-CI-INC: fire-fighting. The installation of fire-safety equipment is obligatory. Procedures for responding to a fire are defined and drilled regularly. The technical rooms must be clean. No cardboard, paper or other flammable material must be stored in these premises.

PHY-CI-EAU: combating water leaks. A study of the risks arising from water leaks must be performed. This study must take particular account of the risk of a leak from a fresh water manifold.

Objective II:

To handle the security of information and communication systems which ensure the safety of a site in a comprehensive manner.

The important sites, recognized if need be as points of vital importance, rely on physical security support services. In this context, the designation 'information and communication systems security services' includes:

- the access control and intrusion detection (CAD) support services, enabling security personnel:
  - to authenticate, authorise and trace access to a physical resource (access control),
  - to detect, alert and trace all attempts at non-authorised access (detection of intrusion).
- the video-surveillance support services (VS), providing security personnel with a camera system covering the whole of the site, a video stream transport system, systems for recording, archiving and viewing these videos;
- the buildings technical management support services (GTB), enabling the supervision and management of all buildings' equipment on-site, and an overview of the condition of these buildings;
- the fire safety support services (INC), including all IT resources deployed to detect, inform, intervene or evacuate all or part of the site in case of fire.

PHY-SI-SUR: securing secure information systems. For the physical sites considered important, protective measures must be defined and applied based on the conclusions of the risk assessment. The risk analysis leads to the designation of essential components whose protection against malicious acts must be ensured. A system for managing the security of a secure information system, drawing on the ISO 27001 standard, ensures maintenance in a secure condition. The use of labelled security products, when they exist, is highly recommended.

Network security

Objective 12:

To use the infrastructure controlled by the entity, observing the security regulations applied to these elements.

Security of internal networks

RES-MAITRISE: systems authorised on the network. Only the equipment managed and configured by the authorised IT teams may be connected to the entity's local network.

RES-INTERCO: interconnection with external networks. All interconnections between the local networks of an entity and an external network (network of a third party, Internet, *etc.)* must use infrastructures controlled by the entity.

RES-ENTSOR: to set up a network filter for inbound and outbound dataflows. With a view to reducing the possibilities offered to a hacker, the outgoing connections of computers in the internal network must be filtered.

RES-PROT: protection of information. It is mandatory that the Internet is accessed via gateways controlled by the entity. When sensitive information must be transmitted on uncontrolled networks, they must be specifically protected with appropriate encryption.

Objective 13:

To control the interconnections of local networks.
To configure active network equipment in an appropriate manner.

Security of local networks

RES-CLOIS: to partition the information system into subnetworks with homogeneous security levels. By analogy with the physical partitioning of a building, the information system must be divided into zones each presenting a homogeneous level of security.

RES-INTERCOGEO: interconnection of the local geographical sites of an entity. The interconnection of an entity's local networks at local level is only possible if justified by geographical proximity and is subject to the establishment of specific connections and secure gateways.

RES-RESS: compartmentalization of resources in the event that premises are shared. In the event that an entity shares premises with external entities, measures for compartmentalizing computing resources must be put in place. The measures taken must be validated by the accreditation authority if they are not physical.

Objective 14:

Not to prejudice information system security through the deployment of non-supervised access.

Specific access

RES-INTERNET-SPECIFIQUE: the particular case of specific access in an entity. Specific Internet access requiring particular rights for a professional use can only be put in place by a duly justified derogation, on computers that are physically isolated and separated from the entity's network, after prior validation by the accreditation authority.

Objective 15:

To control the deployment, configuration and use of wireless networks.

Security of wireless networks

RES-SSFIL: installing wireless networks. The deployment of wireless networks must be subject to a specific risk assessment. Intrinsic protections are insufficient, and supplementary measures must be taken as part of the defence-in-depth approach. In particular, the network must be segmented, so as to limit the consequences of an intrusion via radio waves to an identified area. Unless specific measures are put in place, the deployment of wireless networks on information systems handling sensitive data is prohibited.

Objective 16:

To configure the mechanisms of switching and routing to protect against attacks.

Securing the mechanisms of switching and routing

RES-COUCHBAS: implementing mechanisms to protect against low-level attacks. Particular attention must be paid to implementing low level protocols, so as to guard against the usual attacks through saturation or cache poisoning. This concerns, for example, the ARP protocol.

RES-ROUTDYN: monitoring routing announcements. When the use of dynamic routing protocols is necessary, this must be accompanied by setting up surveillance of routing announcements and procedures which enable rapid response in the event of incidents.

RES-ROUTDYN-IGP: configuring the IGP protocol in a secure manner. The IGP type dynamic routing protocols must be activated exclusively on interfaces necessary to the construction of the network topology and disabled on the remaining interfaces. Configuring the dynamic routing protocol must be systematically accompanied by a password of the type MESSAGE-DIGEST-KEY.

RES-ROUTDYN-EGP: securing EGP sessions. When setting up an EGP session with an external peer on shared media, this session must be supported by a password of the type MESSAGE-DIGEST-KEY.

RES-SECRET: to systematically modify the default authentication elements of equipment and services. It is imperative that the default passwords are changed, as well as the certificates. The arrangements necessary must be made with the supplier so as to be able to modify the certificates installed by default.

RES-DURCI: hardening the configurations of network equipment. The network equipment, such as routers, must be specifically hardened. Apart from changing passwords and certificates, this particularly includes disabling interfaces and unnecessary services, and setting up the protective mechanisms specified in the control plan.

Objective 17:

To keep a detailed and complete map of the networks and interconnections up to date.

Network mapping

RES-CARTO: drawing up the functional and technical architecture documents. The information system's networked architecture must be described and formalised in architecture and configuration diagrams, maintained during the changes made to the information system. The architecture documents are sensitive and are given appropriate protection. Network mapping forms part of information systems global mapping.

Network security

Objective 18:

To apply the principles of defence-in-depth to the software and hardware architecture of computer centres.

Architecture of computer centres

ARCHI-HEBERG: principles of the architecture of the hosting zone. Generally speaking, the infrastructure architecture of computer centres is designed so as to satisfy all the requirements of availability, confidentiality, traceability and integrity. The defence-in-depth principle must be observed, in particular through the successive establishment of 'demilitarized zones '(DMZ), of secure environments in the hosting zone, dedicated virtual or physical machines, appropriate virtual local area networks (VLAN), a strict filtering of application and administration data flows.

ARCHI-STOCK.CI: storage and backup architecture. The storage and backup network for the needs of computer centres is based on a dedicated architecture.

ARCHI-PASS: Internet gateway. It is obligatory for Internet interconnections to pass through approved national gateways.

Information systems operations

Objective 19:

To define and implement strengthened protection measures for sensitive information.

Protection of sensitive information

EXP-PROT-INF: protection of sensitive information in confidentiality and integrity. Measures must be implemented in order to guarantee the protection of sensitive information in terms of confidentiality and integrity. Where a non-accredited network is used, this information must be encrypted using a labelled encryption means.

Objective 20:

Hardening the configurations of computing resources and monitoring operations carried out on these resources.

Security of computing resources

EXP-TRAC: traceability of operations on the system. Maintenance operations on the entity's computing resources must be traced by the computing department. The traces must be accessible to the local SSI officer for at least a year.

EXP-CONFIG: configuration of computing resources. The operating systems and software must be hardened. The configurations and updates are carried out in strict compliance with the guidance documents or procedures in force in the entity, or, failing that, with those in force at central level.

EXP-DOC-CONFIG: documentation of configurations. The standard configuration of computing resources must be documented and updated for each significant change.

Objective 21:

To authenticate users and control their access to information systems resources in accordance with an explicit authorisation policy.

Logical access control

EXP-ID-AUTH: identification, authentication and logical access control. Access to all non-public resources must require individual identification and authentication of the user. Where sensitive data are accessed, strong authentication methods must be used. To that end, the use of a smartcard must be favoured. Access control must be managed and based on a formalised process coherent with human resources management.

EXP-DROITS: access rights to resources. After determining sensitivity level, the need to circulate and share resources, the rights of access to resources must be managed in accordance with the following principles: need-to-know (each user is authorised to access only those resources to which he/she is explicitly granted access) and least privilege (each user accesses resources with the minimum privileges that will enable him/her to carry out the actions for which he/she has explicit authorisation).

EXP-PROFILS: management of applications access profiles. The applications that handle sensitive data must allow close management through access profiles. The need-to-know and least privilege principles apply.

Authorisation process

EXP-PROC-AUTH: authorisation of user access. All actions authorising user access to an information system resource, whether local or national, must form part of a formalised authorisation process, based on the arrival and departure processes of personnel.

EXP-REVUE-AUTH: review of access authorisations. A review of access authorisations must be carried out annually under the supervision of the RSSI, if need be with the support of the local SSI officer.

Management of authenticators

EXP-CONF-AUTH: confidentiality of authentication information. The authentication information (information systems access passwords, private keys associated to electronic certificates, *etc.)* must be considered sensitive data.

EXP-GEST-PASS: password management. Users must not store their passwords in plain text, for example in a file, on their workstation. Passwords must not be transmitted on the networks in plain text.

EXP-INIT-PASS: initialization of passwords. Each user account must be created with an initial random password. If circumstances require, a simpler but single-use password may be considered.

EXP-POL-PASS: password policy. Password management and protection regulations follow the recommendations of ANSSI.

EXP-CERTIFS: use of electronic certificates. The administrative authorities within the meaning of the ordinance No. 2005-1516 of 8 December 2005 apply the regulations of the

Security Reference Documentation (RGS) for electronic certificates. Other entities follow these regulations.

EXP-QUAL-PASS: systematic control of password quality. Technical means enabling the imposition of password policy, for example to check compliance with a possible requirement relating to the use of special characters, must be put in place. Failing that, a regular check of the technical parameters relating to passwords must be conducted.

Management of administrator authenticators

EXP-SEQ-ADMIN: sequestering administrator authenticators. The authenticators enabling the administration of information systems resources must be sequestered and kept updated, in a safe or a locked cabinet. The authenticated administrator must be informed of the existence of these management operations, their purpose and their limits. All administrator access to an IT resource must be traceable and be capable of being traced back to the person exercising this right. Authentication information that has a means of physical protection, particularly smartcards, do not need, by default, to be sequestered by persons other than the authenticated administrator himself/ herself.

EXP-POL-ADMIN: password policy for administrators. All administrators must have a personal password dedicated to administration.

EXP-DEP-ADMIN: managing the departure of an information system administrator. In the event that an administrator who has privileges on information systems components leaves, his/her individual accounts must be immediately disabled. The possible administrator passwords that he/she knows must be changed, for example the passwords of functional accounts, generic accounts or service accounts used as part of administrator functions.

Objective 22:

To provide administrators with the tools necessary for carrying out SSI tasks and to configure these tools in a secure manner.

Systems administration

EXP-RESTR-DROITS: restriction of rights. Apart from exceptions duly justified and validated by the RSSI, users do not have administrative rights.

EXP-PROT-ADMIN: protection of access to administrator tools. Access to administrator tools and interfaces must be limited strictly to persons authorised in accordance with a formal procedure for access authorisation.

EXP-HABILIT-ADMIN: authorisation of administrators. Authorisation of administrators is carried out in accordance with a procedure validated by the accreditation authority. The number of persons authorised for administrator operations must be known and validated by the accreditation authority.

EXP-GEST-ADMIN: management of administrator activities. Administrator operations must be traced in such a way that administrator actions are individually attributable.

EXP-SEC-FLUXADMIN: securing administrator flows. Administrator operations on an entity's local resources must be based on secure protocols. A network dedicated to the administration of equipment, or at the very least a network with logical separation from that of users, must be used. There must be dedicated administrator workstations with no Internet access.

EXP-CENTRAL: centralising management of the information system. In order to effectively manage a large number of user workstations, servers or networked equipment, the administrators must use centralised tools, enabling the automation of day-to-day activities and offering a global and clear view of the information system.

EXP-SECX-DIST: securing of remote control tools. Remote control of a local computing resource must only be possible for agents authorised by the local information systems team, on computing resources in their area. Specific security measures must be defined and observed.

Domain administration[10]

EXP-DOM-POL: defining a domain accounts policy. A clear policy for managing domain accounts must be established.

EXP-DOM-PASS: configuring the strategy for domain passwords. The policy for password management must be designed so as to protect against dictionary attacks. A minimum level of complexity in the selection of passwords must be imposed on users.

Account Management

EXP-DOM-NOMENCLAT: defining and applying a domain accounts nomenclature. Account management must use an appropriate nomenclature, in order to be able to differentiate standard user accounts, administrator accounts (domain, servers, workstations) and service accounts according to their use.

EXP-DOM-RESTADM1N: maximum restriction of domain administrator group membership. Affiliation to the domain groups ENTERPRISE ADMINS and DOMAIN ADMINS is only necessary in rare cases. The most common operations must be carried out with domain accounts that are members of local computer administrative groups or that have delegated administration.

EXP-DOM-SERV: controlling the use of service accounts. Service account passwords are often hard-coded in applications or systems. This bad practice does not allow passwords to be changed, for example in an emergency. So it is necessary to ensure that their use can be controlled.

EXP-DOM-LIMITSERV: limiting the rights of service accounts. Service accounts must be subject to restriction of rights, following the principle of least privilege.

EXP-DQM-OBSOLET: disabling obsolete domain accounts. It is necessary to immediately disable, even delete, obsolete accounts, whether these are user accounts (administrator,

[10] The domain concept is used here in its general meaning, that is a grouping of equipments. For example, in a Microsoft architecture, it is likely to involve a grouping of machines sharing directory information.

service or standard user) or computer accounts.

EXP-DOM-ADMINLOC: improving the management of local administrator accounts. In order to prevent reusing the hashes of a local user account from one computer to another, it is necessary either to use different passwords for local administrator accounts, or to prohibit remote connection via these accounts.

Sending equipment for maintenance and scrap

EXP-MAINT-EXT: external maintenance. Unencrypted data must be deleted before sending any computing resource for external maintenance. The encryption operations must be carried out with labelled security products. The deletion of sensitive data must be carried out with labelled security products or must follow the procedures established in conjunction with ANSSI.

EXP-MIS-REB: scrapping. When a computing resource leaves the entity permanently, the data present on the hard disks or in the integrated memory must be deleted in a secure manner. The deletion of sensitive data must be carried out with labelled security products or must follow the procedures established in conjunction with ANSSI.

Combating malicious code

EXP-PROT-MALV: protection against malicious code. Software protecting against malicious code, commonly called antivirus software, must be installed on all of the entity's gateway servers, application servers and workstations. Distinct protective software must be used for these three categories at least and their logs must be correlated.

EXP-GES-ANTIVIR: managing antivirus security events. Antivirus security events must be sent to a national server for statistical analysis and *a posteriori* problem management (examples: a server that is constantly infected, a virus detected and not eradicated by the antivirus software, *etc.).*

EXP-MAJ-ANTIVIR: keeping the signature database updated. Updating the antivirus databases and the antivirus engines must be deployed automatically on the servers and workstations using a system prescribed by central services.

EXP-NAVIG: configuration of the Internet browser. The browser deployed by the local information systems team on all servers and workstations requiring Internet or Intranet access must be configured in a secure manner (disabling unnecessary services, cleaning the certificate store, *etc.).*

Updating systems and software

EXP-POL-COR: defining and implementing a policy of monitoring and applying security patches. Maintenance of the security level of an information system requires organised and appropriate management of security updates. A management process for patches suitable for each system or application must be defined and adapted to the system's constraints and exposure level.

EXP-COR-SEC: deployment of security patches. The security patches of local computing resources must be deployed by the local information systems team following recommendations made by central services with tools recommended by these services.

EXP-OBSOLET: handling the migration of obsolete systems. All software used on the information system must be in a version which is supported and updated by the editor. In the

event of support malfunction, the impact should be studied and appropriate measures taken.

EXP-1SOL: isolating remaining obsolete systems. It is necessary to isolate obsolete systems, which are kept to expressly to ensure the maintenance of projects in operational condition and for which migration is not practicable. Wherever possible, this isolation must be carried out at network level by stringent filtering, at authentication level, where details must not be the same as the rest of the information system, and at application level (no resource should be shared with the rest of the information system).

Logging

EXP-JOUR-SUR: "logging" alerts. Each system must have "logging" devices which enable the retention of traces of security events. These traces must be preserved in a secure manner.

EXP-POL-JOUR: defining and implementing a policy of management and analysis of trace logs. A policy for the management and analysis of trace logs of security events is defined by the RSSI, validated by the accreditation authority and implemented. The security level of an information system depends largely on the ability of its operators and administrators to detect errors, malfunctions and illicit access attempts occurring on the elements comprising it.

EXP-CONS-JOUR: preserving logs. The security event logs must be preserved on a rolling 12-month basis, excluding particular legal and regulatory constraints imposing specific preservation periods.

Objective 23:

Defending information systems requires the vigilance of all and continuous action.

Defence of information systems

EXP-GES-DYN: dynamic management of security. The team responsible for SSI must set about monitoring abnormal behaviour in the information system and information system inbound and outbound data flows, particularly via the analysis of logs.

Management of computer equipment supplied to users

EXP-MAIT-MAT: control of equipment. Workstations, including hired equipment, are supplied to the user by the entity, managed and configured under the responsibility of the entity. The connection of equipment that is not controlled, administered or updated by the entity, to equipment and professional networks is forbidden, whether this be a smartphone, nomad or fixed computer equipment, or removable storage devices.

EXP-PROT-VOL: review of anti-theft protective measures. Under the current PSSI, all fixed workstations must be physically protected. Each user must ensure the security of removable devices (USB drives and removable disks) in particular by storing them in a secure place. It is recommended that the data contained on these devices be encrypted. Devices containing sensitive data must be stored in units that can be locked with a key.

EXP-DECLAR-VOL: declaring losses and thefts. All losses or thefts of an information system resource must be reported to the RSSI.

EXP-REAFFECT: reassignment of computing equipment. A management procedure for workstations and devices in the context of personnel departures or reassignment to new users must be set up and validated by the RSSI. It must define the conditions under which there is recourse to deletion of data.

Nomadism

EXP-NOMAD-SENS: declaration of mobile equipment suitable for processing sensitive information. The information systems accreditation authority validates the possible use of mobile equipment with regard to the processing of sensitive information; use which is not explicitly authorised is forbidden.

EXP-ACC-DIST: remote access to the organisation's information system. The administrative authorities as defined in ordinance No. 2005-1516 of 8 December 2005, apply the regulations of appendix B3 of the General Security Reference Documentation (RGS) on the authentication of remote users. Other entities follow these regulations.

Securing printers and multifunction copiers handling sensitive information

EXP-IMP-SENS: printing sensitive information. Printing sensitive information must be carried out following a previously defined procedure, guaranteeing control by the user, from the activation of the printing process to collecting the printed material.

EXP-1MP-2: security of printers and multifunction copiers. Printers and multifunction copiers are fully fledged computing resources and must be managed as such. They must not be able to communicate with the outside world.

Objective 24:

To operate computer centres in a secure manner relying on appropriate procedures and control of monitoring tools.

Security of computing resources

The following regulations are presented in accordance with the three-tier model of application architecture (presentation – application – data).

EXP-CI-OS: operating systems. The operating systems deployed must have valid support from an editor or a service provider. Only the services and applications necessary are installed, so as to reduce the attack surface. Particular attention must be paid to the administrator accounts.

EXP-CI-LTP: software in the presentation tier. The implementation of a hardened configuration in software deployed in the presentation tier is mandatory (examples: Web server, Reverse Proxy).

EXP-CI-LTA: software in the application tier. Secure development and configuration regulations for software in the application tier must be settled and applied.

EXP-CI-LTD: software in the data tier. Very stringent regulations (access restrictions, prohibited connections, management of privileges) are applied to software in the data tier.

EXP-CI-PROTFIC: file exchange gateway. File exchange between applications must favour secure protocols (SSL/TLS, FTPS, *etc.).*

EXP-CI-MESSTECH: technical messaging. To meet the needs of infrastructure and application operation and supervision, technical messaging can be deployed in the *"back-office"* area of the computer centre. This technical messaging must in no case be used directly by a user.

EXP-CI-FILT: filtering application flows. So as to guarantee a satisfactory level of security to protect against cyberattacks, filtering and compartmentalization mechanisms must be implemented.

EXP-CI-ADMIN: administrator flows. Generally speaking, two types of administrator flow should be distinguished: infrastructure administrator flow, reserved for computer centre officials, and business application administrator flow, reserved for the core business department. Allocation of administrative rights must respect this differentiation. As far as possible, the two types of administrator flow must be segregated.

EXP-CI-DNS: domain name service - technical DNS. In the event of the deployment of a domain name server to meet internal technical needs in the computer centre, DNSSEC security extensions will be used.

EXP-CI-EFFAC: erasing data from media. The reconditioning and reuse of hard disks for another use, for example the reallocation of a computer or a server, are authorised only following the secure deletion of data.

EXP-CI-DESTR: destruction of storage media. The end-of-life of a device or equipment in which a medium of storage is embedded (printer, router, switch, *etc.)* must be coupled with a destruction operation before restoring factory settings.

EXP-CI-TRAC: traceability and accountability. In order to ensure coherence in exchanges between applications and clear traceability of technical events and security, operating centres use a common time reference (NTP service, Network Time Protocol).

EXP-CI-SUPERVIS: supervision. Supervisory flows (upward flow of information) and administrator flows (command lines, updates) must be seggregated.

EXP-CI-AMOV: access to removable peripherals. Access to removable computer devices is subject to appropriate processing, more particularly when these devices are used to store sensitive information or when they are used for operational activities.

EXP-CI-ACCRES: access to networks. In a computer centre, physical control of access to networks, assignment of IP addresses, filtering of information and the use of specific devices (virtual machines, remote management cards, *etc.)* are subject to secure procedures.

EXP-C1-AUDIT: audit and control. The RSSI directs regular audits of the information systems falling within his/her responsibility.

Workstation security

Objective 25:

To harden the configurations of workstations while protecting users.

Provision of workstations

PDT-GEST: provision and management of workstations. Workstations used professionally are provided and managed by the local information systems team.

PDT-CONFIG: document the configuration of workstations. A formalised procedure for configuring workstations is established by each entity, in compliance with ANSSI recommendations.

Physical security of workstations

PDT-VEROUIL-FIXE: securing the central unit on fixed workstations. When the central unit of a fixed workstation is small, therefore able to be carried away easily, it must be attached to protect it from theft, for example by an anti-theft cable.

PDT-VEROUIL-PORT: securing portable workstations. A physical security cable must be supplied with each mobile workstation. The users must be made aware of its use.

Reallocation of the workstation and recovery of information

PDT-REAFFECT: reallocation of the workstation. An SSI procedure defines the regulations relating to how information which has been stored or handled on reallocated workstations should be processed.

Management of privileges on workstations

PDT-PRIVIL: user privileges on workstations. The management of user privileges on their workstations must follow the principle of least privilege: each user must have only the privileges necessary to conduct the actions falling within his/her remit.

PDT-PRIV: use of administrator access privileges. Administrator access privileges must be used solely for the administrative actions that require them.

PDT-ADM-LOCAL: management of the local administrator account. Access to the local administrator account on workstations must be strictly limited to the teams responsible for the operation and support of these workstations.

Protection of information

PDT-STOCK: storage of information. As far as possible, the data handled by users must be stored on the network in spaces that are backed up according to the requirements of entities and in accordance with the security regulations in force.

PDT-SAUV-LOC: backup and synchronisation of local data. In the event that data must be stored locally on the workstation, users must be provided with the means to backup or synchronise data.

PDT-PART-FIC: file sharing. Sharing directories or databases hosted locally on workstations is not authorised.

PDT-SUPPR-PART: data erasure on shared workstations. The data present on shared workstations (a loaned laptop for example) must be deleted between two uses, as soon as the users do not have the same need-to-know.

PDT-CHIFF-SENS: encryption of sensitive data. An approved encryption method must be made available to users and administrators in order to encrypt sensitive data stored on workstations, servers, workspaces or removable devices.

PDT-AMOV: provision of removable storage devices. Removable storage devices (particularly USB drives and external hard drives) must be supplied to users by the local information systems team.

Nomadism

PDT-NOMAD-ACCES: remote access to the entity's information systems. Remote access to the entity's information systems (referred to as 'nomad' access) must operate via trustworthy virtual private networks (VPN) that comply with ANSSI recommendations.

PDT-NOMAD-PAREFEU: local firewall. A local firewall compliant with ANSSI recommendation must be installed on mobile workstations.

PDT-NOMAD-STOCK: local storage of information on mobile workstations. Local storage of information on mobile workstations must be limited to what is strictly necessary. It is obligatory to encrypt sensitive information using an labelled encryption method.

PDT-NOMAD-FILT: privacy filter. For mobile stations handling sensitive data, a privacy filter must be supplied and fitted to the screen whenever the station is used outside the entity.

PDT-NOMAD-CONNEX: configuration of wireless interfaces. The configuration of wireless interfaces must not allow hazardous uses of these interfaces.

PDT-NQMAD-DESACTIV: disabling wireless interfaces. Configuration regulations for wireless interfaces (Wifi, Bluetooth, 3G, *etc.)*, must be defined and applied, enabling the prohibition of uncontrolled use and the avoidance of intrusion via these interfaces. Wireless interfaces must be activated only in case of need.

Objective 26:

Configure the printers and multifunction copiers in order to reduce their attack surface.

Securing printers and multifunction copiers

PDT-MUL-DUR.CISS: hardening printers and multifunction copiers. The printers and multifunction copiers hosted locally in an entity must be subject to hardening in terms of security: changing the manufacturer's default passwords, disabling unnecessary networked interfaces, deleting unnecessary services, encrypting data on the hard disk when this functionality is available, static network configuration.

PDT-MUL-SECNUM: securing the scanning function. When it is activated, the scanning function on multifunction copiers hosted in an entity must be secured. The following security measures must in particular be applied: sending documents only to an internal address within the entity, sending to a single address.

Objective 27:

Securing telephony to protect users against malicious attacks.

Securing telephony

PDT-TEL-MINIM: securing the configuration of automatic switchboards. The automatic switchboards must be kept updated with regard to security patches. Their configuration must be hardened. The definition and allocation of access rights and privileges to users (outgoing to outgoing transfer, call intrusion, intercoms, unblocking authorisation, call forwarding to an external number, substitution, substitution of privilege, directed call pickup, *etc.)* must be the subject of particular attention. A review of telephone programming must be organized periodically.

PDT-TEL-CODES: telephone access codes. It is necessary to make users aware of the need to change the access code of their telephone and voicemail.

PDT-TEL-DECT: limiting the use of DECT. Communications carried out using the DECT protocol are capable of being intercepted, even if the authentication and encryption mechanisms this protocol offers are activated. It is recommended that users who handle the most sensitive discussions be allocated landlines.

Objective 28:

To regularly check the compliance of the security configurations applied to workstations.

Compliance checks

PDT-CONF-VER1F: using automatic compliance verification tools. A tool for regular verification of the compliance of workstation configuration elements must be put in place, in order to avoid a deterioration of these configuration elements over time.

Security of systems development

Objective 29:

To recognize security as an essential function and to take it into account in the project design stage.

Systems development

DEV-INTEGR-SECLOC: to integrate security into local developments. All local initiatives in computer developments must observe the ANSSI recommendations concerning the inclusion of security in projects and computer developments. The department initiating the project holds itself guarantor that the General Security Reference Documentation (RGS) and a system accreditation procedure will be applied.

DEV-SOUS-TRAIT: integrating SSI clauses into computer development subcontractor contracts. Several clauses relating to SSI must be integrated into subcontractor development contracts:

- obligatory training of the developers in secure development and in the classic vulnerabilities;
- obligatory use of tools to minimise errors introduced during development (free static code analysis tools, use of libraries reputed for their security, *etc.)*;
- production of technical documentation describing the implementation of the protective measures developed (authentication management, password storage, rights management, encryption, *etc.)*;
- compliance with secure development standards, whether these are the developer's own standards, public standards or those of the sponsor;
- obligation on the part of the service provider to correct, within a reasonable time frame and for a defined price, vulnerabilities introduced during development and brought to his/her attention, with automatic inclusion of corrections of other instances of the same programming errors.

Objective 30:

To conduct software development using a methodology that will secure the code produced.

Development of software and security

DEV-FUITES: limiting information leaks. Leaks of technical information on the software used enable hackers to detect possible vulnerabilities more easily. It is imperative that circulation of information about the products used is strictly limited, even if this precaution is not protective in itself.

DEV-LOG-ADHER: reducing the reliance of applications on specific products or technologies. The functioning of an application is dependent on a software and hardware environment. In the design and technical specification phases, it is necessary to check that the applications do not rely too strongly on the environments in which they are based. In effect, the appearance of faults in an environment has an actual impact on the security of the applications which rely on it. In addition to tailored maintenance of the application in a secure condition, it is therefore necessary to be able to update its environment to ensure its security over the long-term.

DEV-LOG-CRIT: establishing secure development criteria. Once past the phases of requirement definition and application architecture design, the level of security of an application depends heavily on the practical modalities followed during its development phase.

DEV-LOG-CYCLE: integrating security into the software life cycle. Security must be integrated into all stages of the project, from the expression of requirements to application maintenance, and including specifications drafting and the acceptance phases.

DEV-LOG-WEB: improving the inclusion of security in Web development. Web development, in particular in PHP, is subject to recurrent security problems which have led to the establishment of security reference documents. These documents aim to establish the rules of good practice for developers. These are generic rules or may be language-specific (PHP. ASP. NET, *etc.).*

DEV-LOG-PASS: hashing passwords in a secure manner. When an application has to store its user passwords, it is important to implement measures to guard against documented types of attack: dictionary attacks, ‘rainbow table’ attacks, brute-force attacks, *etc.*

Objective 31:

To support the secure development of at-risk applications by counter-measures minimising the impact of new attacks.

At-risk applications

DEV-FILT-APPL: implementing application filtering functionalities for at-risk applications. When dealing with at-risk applications, it is recommended that a third-party application filtering solution be used.

Incident handling

Objective 32:

To share information (alerts, incidents) respecting the regulations of rules and to share system recovery operations, so as to combat attacks effectively.

Operational chains

T1-OPS-SS1: SSI operational chains. Alerts and incidents are managed in accordance with procedures tested during exercises. Coordination of expertise is organised at entity level. Emergency situations may call upon measures defined previously during planning.

Processing security alerts issued by national bodies (ANSSI).

TI-MOB: mobilisation in the event of an alert. In the event of a security alert identified at national level, the RSSI of each entity checks that the requirements formulated by national bodies are applied correctly, as quickly as possible.

Reporting security incidents encountered

TI-QUAL-TRAIT: classifying and handling incidents. The SSI functional chain is informed by the operational chain of all security incidents and participates as necessary in classifying incidents and directing their management.

TI-INC-REM: reporting incidents. All security incidents, even apparently minor, whose impact goes beyond, or has the possibility of going beyond an entity's information system, forms the subject of a report, via the SSI chain, to the ANSSI operational centre for information systems security (COSSI).

The reporting of incidents by operational chains is part of an approach based on constant vigilance. Reports of incidents which may impact outside the entity in the short-term and reports of incidents corresponding to specific alerts, particularly from ANSSI, are made immediately. For other incidents, reports take the form of a monthly summary.

The precise criteria and procedures for reporting incidents are developed under the direction of the SSI functional chain in conjunction with the operational chain.

Each entity must maintain a precise updated history of the consequences of each incident, in order to capitalize on information drawn from the resolution or non-resolution of these incidents.

The difficulty in characterising attacks (doubt as to the source, damage caused, method, purpose) makes information exchange necessary, even concerning 'weak signals' as well as the continuous coordination of actions.

Business continuity

Objective 33:

To elaborate business continuity plan and to test them.

Buisiness continuity management of information systems

PCA-MINIS: definition of the plan for the continuity of information systems activity. Each entity defines a plan for the continuity of information systems activity enabling information system activity to continue in the event of a disaster.

Definition of the business continuity plan of an entity's information systems

PCA-LOCAL: defining the local business continuity plan of information system. The entity's director of information systems or the RSSI defines the structure and the objectives of the business continuity plan for the continuity of information systems activity, ensuring effectively that activity will continue in the event of a disaster.

Implementation of the local business continuity plan of information systems

PCA-SUIVILOCAL: monitoring implementation of the local business continuity plan of information systems. The entity's RSSI checks that the provisions laid out in the business continuity plan of information systems are implemented correctly.

PCA-PRQC: implementation of technical measures and operational procedures. The IT teams implement the technical measures and operational procedures that contribute to the continuity of information systems. They handle their day-to-day supervision and maintenance over time.

PCA-SAUVE: protecting the availability of backups. Backed up data must not be subject to the same risks of damage as data in current use.

PCA-PROT: protecting the confidentiality of backups. Backups must be processed in such a way that their confidentiality and integrity is guaranteed.

Maintenance in operational condition of the local business continuity plan of information systems

PCA-EXERC: drilling the local plan for the continuity of information systems activity on a regular basis. The entity's RSSI organises regular exercises, in order to test the local business continuity plan of information systems.

PCA-MISAJOUR: updating the local plan for continuity of information systems activity. The entity's RSSI handles the updating of the local business continuity plan of information systems.

Compliance, audit, inspection, checks

Objective 34:

To carry out checks (audits, inspections) and regular exercises so as to measure progress made and to correct any shortfalls.

Checks

CONTR-SSI: local checks. Compliance of the entity with the PSSI is verified by regular checks. The RSSIs of each entity take action locally to assess compliance with the PSSI and they contribute to the consolidation of progress in its implementation in an annual assessment.

Appendix 2 - Different classes of network

A class 0 network is a public network (Internet, *etc.)* or a network connected to a public network which does not comply with the requirements of class 1 presented below.

A class 1 network is a network which is isolated from all class 0 networks by filtering and flow-break devices as follows[11]:

- at the least, a filtering device qualified at standard level is interposed in all flows to and from class 0 networks;
- a device to interrupt all flows (proxy) to and from the class 0 network, if possible qualified at basic level, is positioned between two filtering devices;
- a sensing probe qualified at least at basic level checks all flows exchanged with the class 0 network.

Interconnections between class 1 networks are authorised[12]. The definition of the interconnection gateway is the responsibility of the entities concerned. The interconnection is subject to an accreditation process distinct from that for networks.

A class 2 network is a network which:

- is isolated, that is not connected, even indirectly, to the Internet;
- does not incorporate any 'descending' interconnection[13] enabling flows to be sent to class 0 or class 1 networks in plain text or encrypted, except by using devices authorised specifically for this use;
- may include 'rising' interconnections enabling the reception of flows from class 0 or 1 networks across a diode authorised by ANSSI for such use.

Interconnections between class 2 networks are authorised[14]. The definition of the interconnection gateway is the responsibility of the entities concerned. The interconnection is subject to an accreditation process distinct from that for networks.

[11] See the ANSSI technical note on its website: " Définition d'une architecture de passerelle d' interconnexion sécurisée" presenting the principles for the design of interconnection devices.

[12] The interconnection is authorised including via a class 0 network when in-line encryption equipment approved by ANSSI is used (see article 14).

[13] A descending flow is a flow originating from a class 2 network sent to a lower class network; a rising flow is the opposite, a flow sent to a class 2 network from a lower class network; it does not involve a transit flow between two components of a class 2 network, across a lower class network.

[14] The interconnection is authorised including via a class 0 network when encryption equipment approved by ANNSI is used in-line (see article 14).

Appendix 3 - Reference documents

Diffusion Restreinte wording and foreign equivalents

General Inter-Ministerial Directive No. 1300/SGDSN/PSE/PSD on the protection of national defence secrecy (IGI No. 1300), approved by the order of 30 November 2011.

General Inter-Ministerial Directive No. 2100/SGDN/SSD of 1st December 1975 on the protection in France of classified information of the North Atlantic Treaty Organisation (IGI No. 2100).

General Inter-Ministerial Directive No. 2102/SGDSN/PSE/PSD of 12 July 2013 on the protection in France of classified information of the European Union (IGI No. 2102).

Protection of the Nation's scientific and technological potential

Decree No. 2011-1425 of 2 November 2011 in application of article 413-7 of the penal code and pertaining to the protection of the Nation's scientific and technological potential.

Order of 3 July 2012 pertaining to the protection of the Nation's scientific and technological potential.

Inter-Ministerial circular on the implementation of the system for protection of the Nation's scientific and technological potential, of 7 November 2012.

General Security Reference Documentation (RGS)

Ordinance No. 2005-1516 of 8 December 2005 pertaining to electronic exchanges between users and the administrative authorities and between administrative authorities.

Decree No. 2010-112 of 2 February 2010 implementing articles 9, 10 and 12 of the Ordinance No. 2005-1516 of 8 December 2005.

Order of 13 June 2014 in application of RGS V2 specifying the modalities for implementing the procedure for validating electronic certificates.

Security policy for State information systems

Circular of the Prime Minister No. 5725/SG of 17 July 2014 on security policy for State information systems.

ANSSI Guidance documents

Guidance document on computer hygiene.

Guidance document "Security accreditation in nine simple steps".

Technical note "Definition of a secure interconnection gateway architecture". Guidance document "Controlling risks associated with managed services - Outsourcing information systems". Guidance to development of information systems security policies.