



Policy defining the terms of use for information technology (IT) resources and access to digital networks provided by the CNRS, hereinafter the

IT Policy

This IT Policy establishes the rights and obligations of Users when utilizing IT Resources or accessing Digital Networks provided by CNRS.

It reflects CNRS' commitment to protecting its intangible assets and information against any deliberate or accidental breach of confidentiality, integrity, or availability, while safeguarding its reputation and legitimate interests. Such breaches may have significant human, financial, legal, reputational, environmental, or operational consequences, or impact CNRS' scientific and technical potential.

CNRS implements technical and organizational measures to ensure the security of IT Resources and access to Digital Networks provided to Users.

Users must comply with the terms of this IT Policy, as well as general regulations and specific IT Security rules referenced in the decision approving the IT Policy, the *Politique générale de sécurité de l'information (PGSI)*, and the *PSSI opérationnelle (PSSIO)* in effect within the Entity.

Users are responsible for the security of IT Resources provided by CNRS for their use. They may rely on the Local/Laboratory IT Security Officer (« *Chargé de la sécurité des systèmes d'information (CSSI)* ») or the CNRS Regional IT Security Officer (« *Responsable de la sécurité des systèmes d'information en délégation régionale (RSSI-DR)* ») for assistance and to address questions. Users must report any incident, malfunction, or unusual event to their *CSSI*, *RSSI-DR*, and direct supervisor. If personal data is involved, the incident must also be reported to the competent Data Protection Officer (DPO). The *Coordination Nationale pour la SSI (CNSSI)*, under the direction of the National Chief IT Security Officer ("*RSSI National (RSSI-N)*"), manages relations with joint laboratory's affiliated Institutions (*les tutelles*), national partners, and public agencies. It also oversees the functional chain of IT security within CNRS.



Contents page

I. Definitions	4
II. Applicable regulatory framework.....	4
III. Protection of IT Equipment	5
a) Protection of authentication methods.....	6
b) Terms of use for IT system and network access rights	6
c) Prohibition of free digital services.....	7
d) Purpose of IT Resource usage	7
V. Protection of information/data contained in IT Resources	7
VI. Protection of digital correspondence	8
a) Email address and associated mailbox.....	9
b) Content of digital correspondence	9
c) Publishing information on institutional websites.....	10
d) Videoconferencing and instant messaging	11
e) Vigilance regarding received information	11
VII. Use of Artificial Intelligence technologies.....	11
VIII. Remote work.....	11
IX. On field mission.....	11
X. Privacy and personal IT Resources	12
a) Residual personal use.....	12
b) Personal IT Resources	12
XI. Employee offboarding process.....	13
XII. Protection of personal data.....	13



XIII. Respect for intellectual property	13
XIV. Traceability of user activities	14
XV. Special provisions for privileged IT system employees.....	14
a) Administrator prerogatives	14
b) Administrator obligations	15



I. Definitions

Administrator: Technical (System and Network Administrator, IT technician, etc.) or functional (application owner, access rights administrator, etc.) personnel with elevated privileges and broad access to CNRS IT systems and/or data, as defined in their job description or specific mission.

CNSSI (National Chief IT Security Officer): The service responsible for defining and supporting the implementation of CNRS's national IT Security Policy and ensuring compliance with regulations (contact: cnssi@cnrs.fr).

CSSI (Local/Laboratory IT Security Officer): The ISS officer for the Entity.

Data Encryption: Mathematical transformation of data to render it unreadable to unauthorized parties, ensuring confidentiality, integrity, authenticity, and protection against theft or leaks. Decryption requires a secret code known only to the User.

Data Protection Officer (DPO): Responsible for ensuring compliance with the GDPR for personal data processing by CNRS and its Entities (contact: dpd.demandes@dpd-cnrs.fr).

Digital Networks: All electronic communication networks accessed by Users, whether local (within an Entity) or external, including Internet usage.

Entity(ies): All entities created by CNRS to fulfill its missions, including laboratories under its supervision, administrative services, and departments.

IT Equipment: Any device provided to the User for storing or processing digital data, such as laptops, workstations, screens, external storage media (magnetic/optical disks, USB drives, flash memory, etc.), smartphones, tablets, authentication devices, etc.

IT Resources: All IT means for storing, processing, and transferring digital data (IT Equipment, information systems, servers, applications, websites, Internet access, networks, etc.) provided by CNRS to the User for their professional activities, whether on-site or remotely.

RSSI-DR (Regional IT Security Officer): The regional IT representative, a member of the IT functional chain, hierarchically attached to the regional delegate and functionally to the CNSSI.

User(s): CNRS Entity employees, as well as individuals or legal entities hosted or welcomed within an Entity (visitors, service providers, etc.) who have access to IT Resources provided by CNRS.

II. Applicable regulatory framework

In addition to the texts governing the IT Security Policy ¹, Users must comply with the following regulations (non-exhaustive list) when using IT Resources or accessing Digital Networks provided by CNRS:

- Ethical obligations under articles L121-1 to L121-11 of the *code général de la fonction publique*.

¹ See also: <https://securite-si.cnrs.fr/pssi/>



- Articles relating to French Scientific Data and Activities Protection law (*« Protection du potentiel scientifique et technique de la Nation » (PPST)*) (including articles 413-7, 413-8, and R. 413-1 et seq. of the *code pénal*, décret n°2011-1425 du 2 novembre 2011 and arrêté du 3 juillet 2012 modifié relatif à la PPST de la Nation).
- Press freedom of speech law (*« Loi du 29 juillet 1881 modifiée sur la liberté de la presse »*) : Users must not disseminate information constituting attacks on personality (defamation, insult, incitement to discrimination or racial hatred, Holocaust denial, etc.).
- Respect for privacy (article 9 of the *code civil*) and professional secrecy (article L121-6 of the *code général de la fonction publique* and articles 226-13 and 226-14 of the *code pénal*).
- Personal data processing regulations, including the *Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (Loi Informatique et Libertés)* and the General Data Protection Regulation (GDPR) of April 27, 2016.
- IP code (*« Code de la propriété intellectuelle »*).
- Articles regarding offenses against automated data processing systems (articles 323-1 to 323-8 of the *code pénal*).
- Regulation (EU) 2022/2065 of October 19, 2022 (Digital Services Act, DSA), which establishes rules for digital platforms to combat the spread of illegal or harmful content.
- Economical security and trust law (*« Loi n°2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique »*).

Non-compliance with these provisions may result in criminal and/or disciplinary sanctions.

III. Protection of IT Equipment

Users must ensure the protection of IT Equipment provided to them:

- IT Equipment with storage media (workstations, laptops, smartphones, tablets, external storage, etc.) must be encrypted and protected against malware, in compliance with the Entity's PSSI, with support from the CSSI and the Entity's IT service;
- Users must not introduce external storage media (magnetic/optical disks, USB drives, flash memory, etc.) without complying with the Entity's PSSI and must take precautions to ensure their safety, with support from the CSSI and IT service;
- Users must lock or close all active sessions on their workstation in case of absence, even temporarily, and shut down their workstation at the end of the day or in case of prolonged absence;
- Users must use provided hardware protection measures (anti-theft cables, locked drawers/cabinets, etc.) to secure physical access to mobile devices and the information they contain against theft;
- Users must immediately report to the CSSI, RSSI-DR, and/or their direct supervisor any loss, theft, suspected or confirmed compromise of IT Equipment, or any malfunction in security patches or application updates. If personal data is involved, the incident must also be reported to the competent DPO.



In case of theft of CNRS-owned IT Equipment, CNRS is responsible for filing a complaint, in accordance with the *circulaire pénale*².

IV. Protection of authentication methods and terms of use for IT system access rights

Users are responsible for the use of IT systems access via their authentication means and access rights.

a) Protection of authentication methods

Users must protect the authentication means assigned to them or generated by them (badges, passwords, private keys linked to certificates, multi-factor authentication devices, etc.). Users must:

- Never share them with third parties, including supervisors or the Entity's IT service;
- Apply complexity and renewal rules³ in force for the authentication means used;
- Change or request renewal of authentication means if they suspect disclosure, and immediately inform the Entity's *CSSI*, *RSSI-DR*, and direct supervisor;
- Ensure access to professional data, particularly within the data recovery⁴ policy implemented in the Entity.

Users must not use another person's authentication means or attempt to conceal their identity when accessing the IT system.

b) Terms of use for IT system and network access rights

Users may only use their access rights to access information or services necessary for their assigned missions and for which they are authorized.

They do not compromise the IT systems and networks' functioning, the protection measures implemented, or their functionalities.

Hence, Users must not:

- Access or attempt to access IT Resources for which they have not received explicit authorization;
- Connect unauthorized or non-Entity-approved devices to the Entity's local networks (wired or wireless);
- Install, download, or use unlicensed software or software from illegal or prohibited sites on Entity's or personal devices used for professional purposes;
- Use CNRS-licensed software on personal or unauthorized devices;
- In accordance with the provisions of article 323-3-1 of the *code pénal*, use software or tools to test, bypass, or penetrate CNRS IT Resources' security, unless their role requires it (*CSSI*, *RSSI-DR*, *RSSI-N*) and they comply with professional ethics and prior hierarchical approval.

They inform the Administrator of any changes in their duties that require a modification of their access rights.

² Circulaire n°CIR192121DAJ du 30 août 2019 relative à la mise en œuvre de poursuites pénales par le CNRS.

³ https://sesame.cnrs.fr/secure/CHANGE_PASSWORD

⁴ Recovery is the backup mechanism that allows an authorized person to access data when the primary mechanism is no longer usable (for example, if a password is lost).



Access to Restricted Zone (*Zone à régime restrictif*, or *ZRR*) IT systems requires prior authorization, in accordance with applicable regulations and internal rules.

c) Prohibition of free digital services

CNRS prohibits the use of unvalidated free (or low-cost) online services for storing, processing, or disseminating professional information (collaborative work, videoconferencing, data processing, AI, document design assistance, etc.) using IT Resources provided by CNRS.

Such services pose significant risks to data confidentiality and system integrity (embedded ads capturing and monetizing personal data, data analysis and resale to third parties, foreign countries' access to User data, etc.).

Only tools and applications provided or explicitly authorized by CNRS or a co-supervising Institution may be used⁵.

d) Purpose of IT Resource usage

While limited residual personal use may be tolerated, the use of IT Resources provided by CNRS is presumed to be professional. Users must not use their professional contact details (e.g., email address) for services unrelated to their professional activity. Non-compliance may facilitate cyberattacks and harm CNRS' reputation.

In addition, some malicious websites or applications exploit software vulnerabilities to steal data from the user's computer. Other sites offer software that, while appearing harmless or hidden within other programs, can take control of the computer and transmit its contents to the hacker without the user's knowledge.

Additionally:

- Users must not connect to suspicious websites⁶;
- Users must not download or install unvalidated software;
- Backups, information sharing, and collaborative exchanges must only be performed using validated and CNRS-provided devices with attested security (e.g., security certification);
- Encryption of confidential data stored on third-party sites or transmitted via unsecured messaging must be performed using tools provided by CNRS.

V. Protection of information/data contained in IT Resources

Users must be aware of the risks to themselves or the institution arising from their use of IT Resources, including:

- Disclosure of personal data (GDPR and *Loi Informatique et Libertés*);
- Theft or corruption of information produced, processed, or known by the User, left accessible due to negligence or error, or disclosed by the User;
- Loss of scientific or administrative data;

⁵ Refer to : <https://magelan.cnrs.fr>, <https://securite-si.cnrs.fr>, https://intranet.cnrs.fr/Cnrs_pratique/si/Pages/default.aspx

⁶ Websites that display information that is clearly illegal or misleading, or that attempt to take advantage of Internet users' gullibility.



- Abuse or misuse of access to applications and services, particularly following the theft of personal credentials;
- Illegal use of certain information accessible online (images, photos, etc.) in violation of intellectual property rights;
- Disruption of IT Resource operations due to malicious, careless, or untimely third-party actions.

Through vigilance, rigor, and responsibility, Users contribute to mitigating these risks, protecting both the institution and themselves.

Users must comply with the professional data preservation policy defined within the Entity, in accordance with the Patrimonial Code (“*code du patrimoine*”) and in coordination with the archives manager.

If automatic backups are not in place, Users must implement the manual backup system recommended by their Entity.

Note: A sensitive IT processes data whose unauthorized disclosure, alteration, or unavailability could harm the interests of the persons concerned, the proper functioning of the service, or the missions and interests of CNRS and/or its partners, and/or the PPST.

The transmission of sensitive data under the *Instruction interministérielle n°901 du 28 janvier 2015* (unclassified sensitive defense data) or the *Instruction interministérielle n°1300 du 9 août 2021* (information subject to national defense secrecy) is prohibited, except when using ANSSI’ qualified technical solutions.

Users must protect information they handle in their role, according to its sensitivity.

When creating digital content, Users must determine its sensitivity level and apply rules to ensure its protection throughout its lifecycle (labeling, storage, transmission, printing, deletion, etc.). They must follow the information labeling and dissemination rules defined in the Entity’s *PSSI* (or, by default, CNRS’ *PSSI*⁷, PDI-1 and PDI-2 rules).

When processing personal data, Users must comply with personal data protection regulations (GDPR and *Loi informatique et Libertés*), in coordination with the director of the laboratory and the competent DPO.

VI. Protection of digital correspondence

Users must protect their digital correspondence (emails, videoconferencing, social networks, discussion forums, instant messaging, document sharing, recordings, voice, images, videos, etc.).

The *CSSI* or *RSSI-DR* provides support to Users for implementing these measures.

⁷ <https://securite-si.cnrs.fr/pssi/>



a) Email address and associated mailbox

CNRS provides CNRS' employees with a nominative professional mailbox in the "cnrs.fr" domain, enabling them to send and receive electronic messages. Use of this email address is the User's responsibility.

Non-CNRS employees must use the email address provided by their employer, in accordance with its rules.

Users must not use personal email for professional communications or to access CNRS information systems (e.g., as a Janus identifier).

By default, any message sent or received via the professional email provided by the employing administration is presumed to be professional. Thus, CNRS may access the professional emails of its employees without prior consent or the employee's presence, subject to the proper procedure and respect for messages explicitly marked as "private."

If necessary (e.g., departure or prolonged absence), CNRS may access an employee's professional mailbox, provided the messages are not identified as private⁸.

b) Content of digital correspondence

For all digital exchanges (emails, videoconferencing, social networks, forums, instant messaging, document sharing, recordings, voice, images, videos, etc.), Users must comply with applicable regulations, including criminal law (which prohibits, among other things, blackmail or threats, malicious messages, and harassment), laws regarding historical memory⁹, and the *Loi du 29 juillet 1881 sur la liberté de la presse*, as well as the ethical obligations set forth in the *code général de la fonction publique*¹⁰.

Therefore, all Users are required to ensure that they do not post any content:

- promoting fascist, xenophobic, racist, or sectarian ideologies;
- insulting or defamatory within the meaning of article 29 of the *Loi du 29 juillet 1881*;
- infringing on intellectual property rights belonging to third parties;
- insulting, humiliating, or infringing on the privacy, reputation, or presumption of innocence of a third party as defined in articles 9 and 9-1 of the *code civil*;
- containing child pornography;
- likely to constitute unlawful direct or indirect advertising;

⁸ Note DAJ « Cadre juridique applicable et procédure d'accès à la messagerie professionnelle d'un agent CNRS » du 25 octobre 2023.

⁹ These are the following laws :

- Loi du 13 juillet 1990 tendant à réprimer tout acte raciste, antisémite ou xénophobe qui crée le délit de négation du génocide des juifs ;
- Loi du 29 janvier 2001 relative à la reconnaissance du génocide arménien de 1915 ;
- Loi du 21 mai 2001 tendant à la reconnaissance de la traite et de l'esclavage en tant que crime contre l'humanité ;
- Loi du 23 février 2005 portant reconnaissance de la Nation et contribution nationale en faveur des Français rapatriés.

¹⁰ Articles L121-1 et seq.



- inciting the commission of offenses or glorifying offenses within the meaning of article 24 of the *Loi du 29 juillet 1881*;
- denying crimes against humanity and other crimes referred to in article 24 bis of the same law;
- likely to undermine public order, respect for human beings or their dignity, gender equality, or the protection of minors;
- encouraging, containing, or inciting discrimination, insults, hatred, or violence against a person or group of persons, in particular on the basis of their origin, or their membership or non-membership in an ethnic group, nation, race, or religion, their disability, their sexual orientation, or any other difference;
- glorifying, denying, or questioning war crimes and/or crimes against humanity;
- encouraging the commission of crimes or offenses, or the trade and consumption of illicit substances, prostitution, terrorism, sexual assault, theft, suicide, violence, or dangerous property damage, or undermining the authority of the judiciary.

Users must comply with the *Circulaire relative aux conditions d'utilisation des réseaux sociaux au CNRS*¹¹ and the *Charte de l'expression publique des scientifiques du CNRS*¹².

Non-compliance may result in criminal and/or disciplinary proceedings.

Hosting providers must remove manifestly illegal content upon notification, in accordance with article 6 of the Digital Services Act.

Digital exchanges with third parties may have legal probative value and could form a contract under certain conditions.

Users must exercise caution regarding the nature of information exchanged electronically, as with traditional mail.

c) Publishing information on institutional websites

Publishing information on institutional websites, networks, or the Entity's intranet is the responsibility of the publication manager, in accordance with the Entity's internal regulations (*règlement intérieur*) and the *Circulaire relative aux conditions d'utilisation des réseaux sociaux au CNRS*. Publishing illegal content exposes CNRS and the User to liability.

No personal or non-professional information may be published on institutional sites, intranets, or via Entity IT Resources, unless explicitly authorized by the Entity and its the joint laboratory's affiliated institutions.

¹¹ <https://docutiles.cnrs.fr/docutiles/documents/21186>

¹² https://www.cnrs.fr/sites/default/files/news/2025-07/Guide%20de%20l'expression%20publique%20des%20scientifiques%20du%20CNRS_WEB.pdf



d) Videoconferencing and instant messaging

The use of videoconferencing services is governed by CNRS guidelines¹³, which Users must follow. Only recommended tools may be used for professional exchanges. Users, in coordination with the CSSI, must select videoconferencing tools based on the sensitivity of their exchanges.

Recording audio/videoconferences is only permitted with the explicit and traceable consent (written or recorded oral) of all participants. Recordings must be retained only for their administrative usefulness, ensuring confidentiality, and destroyed after the authorized period, in accordance with the *code du patrimoine*.

e) Vigilance regarding received information

Users must exercise vigilance and critical thinking toward digitally received information (disinformation, computer viruses, phishing attempts, chain messages, etc.). Particular caution is required for messages appearing to come from administrative, financial, judicial authorities, or well-known personalities. The same applies to audio or video files, which may be artificial Intelligence -generated (e.g., deepfakes¹⁴). Any doubt must be reported to the direct supervisor and the Entity's IT service for assessment.

VII. Use of Artificial Intelligence technologies

Unless exempted¹⁵, the use of general-purpose generative AI tools (free or paid) by CNRS employees and Entity directors for professional activities — other than CNRS' internal generative AI assistant¹⁶ — is prohibited.

VIII. Remote work

When working remotely, Users must comply with this IT Policy, as well as the Entity director's instructions and the Operational Guide for the Remote Worker ("*Guide opérationnel du télétravailleur*¹⁷"). They must ensure the protection of information processed in this context, where data confidentiality risks are heightened.

Access to the Entity's IT Resources must be done exclusively via VPN (Virtual Private Network) provided by the Entity.

IX. On field mission

Users on field mission face increased risks of loss or theft of the equipment entrusted to them, as well as the risk of a breach of confidentiality regarding the data they carry with them (including, for example, when overseas, in the event that foreign law enforcement or judicial authorities access that data). They should therefore limit the

¹³ https://intranet.cnrs.fr/Cnrs_pratique/si/pratique/Pages/Outils-communication.aspx

¹⁴ A technique based on artificial intelligence that enables the creation of ultra-realistic manipulations (or "hyper-manipulations") of images, videos, and audio for the purposes of fraud, disinformation, and cyberbullying.

¹⁵ To be defined.

¹⁶ https://emmy.cnrs.fr/files/Conditions_utilisation_emmy.pdf

¹⁷ https://intranet.cnrs.fr/Cnrs_pratique/recruter/temps/Documents/Teletravail_guide_operationnel_2023_2.pdf



amount of data they carry to what is strictly necessary and exercise heightened vigilance regarding their equipment for the duration of the mission.

Prior to the field mission, the user should contact the Entity's IT service to review and implement the specific guidelines. In any case, it is recommended to strictly follow ANSSI's guidelines¹⁸.

X. Privacy and personal IT Resources

a) Residual personal use

IT Resources (workstations, servers, applications, digital services, email, Internet access, phones, etc.) provided by CNRS or a co-supervising Institution are reserved for professional use.

Limited personal use is tolerated only if:

- It is brief during working hours;
- It does not interfere with professional use;
- It does not compromise the functioning or security of IT Resources;
- It is not for profit;
- It does not violate regulations or internal rules.

Any message explicitly marked as private (e.g., labeled "Private" in the subject) or stored in a "Private" folder is considered private correspondence, protected by the right to privacy.

Private messages may only be accessed by the employer in the presence of the employee and with their explicit consent.

Users must store private data (files, documents, etc.) in a designated private space or clearly label the resource as private. Professional data must not be stored in this private space. This space must occupy only a minor portion of the allocated IT Resources. The protection, migration, and regular backup of personal data are the User's responsibility.

b) Personal IT Resources

The use of personal IT resources (computers, smartphones, USB drives, external hard drives, tablets, access to external services, etc., purchased with personal funds) for professional purposes is discouraged but may be explicitly authorized by the Entity's director on a case-by-case, temporary, and exceptional basis, provided its use complies with the Entity's security policy.

In Restricted Zones (ZRR), the use of personal equipment is prohibited.

When personal IT resources are used to access CNRS information systems, they must not contravene or weaken the Entity's security policies through insufficient protection or improper use.

¹⁸ [passeport_voyageurs_anssi.pdf](#)



Users must protect personal devices used to access CNRS information systems remotely or from an Entity's local network with the same security measures as professional IT Equipment. In particular, they must ensure:

- Effective antivirus protection,
- Up-to-date software patches,
- No storage of professional credentials on personal devices.

The Entity's IT service may provide assistance for implementation.

XI. Employee offboarding process

Professional data remains the property of the employer. Data preservation policies are defined within the Entity, in accordance with the *code du patrimoine* and in coordination with the archives manager.

Before departure, Users must ensure, in coordination with their supervisor, that the Entity has effective access to the professional data they handled.

Users are responsible for their private data space and must delete it upon departure. In exceptional circumstances (unexpected departure or death), CNRS may store private data spaces on provided IT Resources for a maximum of three months (to allow the User or their heirs to retrieve the information).

In case of death, the deceased employee's supervisor, as the data controller, must verify whether the employee had defined directives regarding the retention, erasure, or communication of their personal data after death. In the absence of such directives, heirs who prove their identity (ID copy and proof of kinship) may exercise certain rights under article 85 of the *Loi Informatique et Libertés*. The decision to communicate the data is assessed on a case-by-case basis.

XII. Protection of personal data

In their activities, Users may process personal data.

They must comply with personal data protection regulations, as well as the procedures implemented by the joint laboratory's affiliated institutions and the operational *PSSI* in effect within the Entity. In particular, they must record the processing activity in the dedicated registry of the Institution. To this end, they must consult the competent DPO.

XIII. Respect for intellectual property

Users must not reproduce, download, copy, distribute, modify, or use software, databases, web pages, images, videos, photographs, or other creations protected by intellectual property rights without prior authorization from the rights holders.



XIV. Traceability of user activities

Regulations require CNRS to maintain a history of accesses to its information systems by Users¹⁹. CNRS has implemented logging of these accesses, in accordance with the *PGSI* and personal data protection regulations.

Administrators have access to the logs generated by Users during their access to all IT Resources provided by CNRS, as well as local and remote networks. These logs (also called "log files" or "journals") are retained for a maximum of twelve months.

In case of technical malfunction, intrusion, or attack attempts, Administrators may use these logs to trace the origin of the incident and mitigate its consequences.

CNRS deploys protection software for IT Equipment against malware and malicious actions, enabling real-time monitoring of IT Equipment activity. If suspicious behavior is detected, the protection software may suspend the connection or activity of the IT Equipment. This software also collects information on IT Equipment behavior and usage, in compliance with applicable regulations²⁰.

XV. Special provisions for privileged IT system employees

a) Administrator prerogatives

In accordance with their assigned instructions, Administrators may take any necessary measures to ensure the proper functioning and security of IT Resources within their scope of responsibility, as defined in their job description or mission letter. In particular, they may, in accordance with professional ethics and regulations:

- Isolate, suspend, or reconfigure user accounts, equipment, or applications that could compromise the IT security. In urgent situations, they must request authorization from their direct supervisor and inform the *CSSI* or *RSSI-DR* in all cases.
- Conduct technical verifications on files, databases, emails, Internet connections, log files, etc., to detect any anomalies or security incidents that could affect the proper functioning and security of IT in administrative and support activities.
- Process (detect, analyze, eradicate, filter, etc.) or ensure the processing of any IT traffic posing security risks (e.g., viruses, intrusions, use of prohibited or potentially dangerous software, etc.). Based on statistical data, Administrators may alert the *RSSI-DR* to any use of IT Resources that appears non-compliant with this Policy or the *PSSI*.

An Administrator who misuses their privileges for purposes other than those authorized commits an offense against automated data processing systems and may face disciplinary and/or criminal proceedings.

¹⁹ Décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, pris en application du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique which requires hosting providers and internet service providers to retain identification data for connections to their services, and article L.34-1 of the *code des postes et des communications électroniques (CPCE)* which imposes an obligation to retain such data.

²⁰ Processing of personal data registered with the CNRS under number 2-25229.



b) Administrator obligations

Administrators must strictly adhere to security rules and the limits of their interventions:

- They must comply with applicable security rules, particularly those protecting the use of privileged accounts and rights assigned to them. They must ensure the protection of workstations from which they perform their duties and the management of privileged account credentials and authentication means. Privileged access is confidential and non-transferable.
- They must limit their actions to the IT Resources under their responsibility and within the scope of their mission. They may only modify configurations and access rights in predefined cases.
- They must not accept instructions from unauthorized persons and must escalate any inappropriate or non-compliant requests to their direct supervisor (as listed in their job description) and the *RSSI-DR*. If a request from their hierarchy seems inappropriate, they must explain their objections. If the request is maintained, they must notify the *RSSI-DR* or *RSSI-N*.

Additionally:

- Controls must be conducted transparently and in a proportionate manner, aligned with the previously communicated purpose to the User.
- Administrators must avoid conflicts of interest and inform their hierarchy of any potential conflicts that could impair their mission's effectiveness.
- They must document their actions and interventions to ensure the proper functioning and continuity of the service.
- They must cooperate with the *RSSI-DR* and follow predefined procedures.

Administrators are bound by confidentiality in their role. Therefore:

- Administrative permissions must only be used to carry out assigned tasks.
- Tools provided must only be used for professional purposes (administration, supervision, operation, maintenance, or support).
- Administrators may access professional information in IT or grant access only within the scope of their duties and/or upon explicit request from their supervisor or, in their absence, the *RSSI-DR* (a brief summary of the action will be recorded).
- They must not access or attempt to access the content of directories, files, or messages explicitly marked as private, except in the presence of the employee and with their explicit consent, in cases of justified emergency or regulatory necessity for IT security.
- In case of remote assistance, they may only take control of a User's workstation with explicit authorization and only access the resources necessary for their mission.



- Duties of reserve and professional secrecy prohibit them from disclosing details of their missions or functions to unauthorized third parties.