ARCAN Recommandations

Suite cryptographique civile, souveraine & protectrice du vivant

Stéphane Valente
www.ariel-ia.ch

Summary

ARIEL-IA Official Recommendations

ARCAN Best Practices

Enterprises, Public Administrations & Organisations

---

1. Preamble

At ARIEL-IA, we have received certain pre-order requests that can be described as fanciful or excessive.
While our objective is indeed to make ARCAN available, we will **never** do so at the expense of our clients, their security, or their internal organisation.

Deploying ARCAN on every workstation within an organisation **can** be a choice.
However, it is **not our recommendation**.

ARCAN is a powerful civil encryption tool.
Its value lies in **controlled and deliberate use**, not in blind generalisation.

---

2. Usage recommendations

As a general rule, ARIEL-IA recommends:

- **A maximum of 1 ARCAN workstation per 10 employees**
- **A clearly designated encryption officer**
- **A formalised internal procedure**, explicitly covering:
    - password storage and management
    - data lifecycle management
    - clearly defined moments when encryption is applied

Encrypting everything, all the time, without a framework is unnecessary and counterproductive.

Security is not achieved through the anarchic multiplication of encryption operations,
but through a **controlled, clearly defined and understood cycle**
(see the recommended usage cycle diagram).

Our interest is not to sell licences at any cost.
Our interest is to protect organisations, administrations, data —
and ultimately, people.

Creating cryptographic chaos would be irresponsible, ineffective,
and contrary to our ethics.

---

3. Support & responsibility

ARCAN is not a tool reserved for engineers or cryptography specialists.
The ARCAN Console has been designed to be usable by any user,
without advanced technical skills.

However, certain rules are non-negotiable:

- The password is under the **exclusive responsibility of the user**
- No trace of the password is stored
- No one can decrypt an ARCAN file without the password
- Neither the development team,
  nor ARIEL-IA,
  nor any authority
  has any recovery access

👉 If the password is lost, the file is permanently lost.
👉 There is no Plan B.

This irreversibility is a deliberate choice,
at the very core of ARCAN's security.

---

4. High-volume use cases

Only organisations handling large volumes of encrypted files
may enable a password export option.

In such cases:

- responsibility for exporting passwords lies **exclusively** with the persons in charge of encryption
- responsibility for storing the password file lies entirely with them
- if this file is lost, the encrypted files are lost

Once again:
👉 no recovery is possible
👉 no exception exists

---

5. Final position

ARCAN is secure by design
and mathematically robust.

ARCAN is **not a toy**.

Its effectiveness relies as much on:

- the quality of its cryptography,
- as on the **human discipline** governing its use.

Official recommendations — ARCAN usage cycle in organisations

🧭 ARCAN Usage Recommendations

Security through responsibility, sovereignty through rigour

Preamble

ARCAN is a sovereign encryption tool designed to provide real and irreversible protection of sensitive data.
It is neither a turnkey product,

nor a magic solution,
nor a substitute for a well-designed security architecture.

The security provided by ARCAN depends as much on its cryptographic design
as on the way it is used.

These recommendations aim to transmit a culture of responsible use,
an indispensable condition for genuine digital sovereignty.

---

1. Fundamental principle: responsibility and restraint

ARCAN is a powerful tool.
As such, its use must be restrained, targeted and controlled.

Multiplying ARCAN-equipped workstations does not mechanically increase security.
On the contrary, each additional instance introduces a new point of human responsibility.

ARIEL-IA explicitly recommends **not** generalising ARCAN installation to all staff.
The more powerful a tool is, the more restricted its use should be.

ARCAN is not intended to become a convenience button distributed to everyone.
It is meant to be entrusted to identified, trained individuals fully aware of the implications of their actions.

2. Recommended organisational structure

Clear human responsibility
ARIEL-IA recommends:

- one to two persons maximum per department or entity
- clearly designated
- explicitly responsible for encryption and its consequences

These individuals are not mere technical operators.
They carry a **functional and organisational responsibility**.

Separation of roles
In a sound organisation:

- document production
- data access
- cryptographic responsibility

do not necessarily need to be combined.

ARCAN follows a role-separation logic to limit human and organisational risks.

3. Recommended hardware architecture

Security by design, not by illusion

Cybersecurity does not begin with software.
It begins with architecture.

ARIEL-IA strongly recommends:

Dedicated external storage

- external drives dedicated to encrypted data
- hot-swappable media
- secured USB keys
- no long-term storage on standard user workstations

Physical protection

- storage of media in fireproof or fire-resistant safes
- physical separation of locations where possible
- clear inventory and tracking of storage media

ARCAN is designed to operate in sober, isolated and controlled environments.
It does not replace a sound architecture — it strengthens it.

4. Password management: seriousness and irreversibility

ARCAN applies a strict and deliberately irreversible security doctrine:

- loss of the password results in permanent data loss
- no recovery is possible
- no exception exists
- no authority can intervene

This reality must be fully understood before any use.

Essential recommendations

- strong and unique passwords
- never stored on connected systems
- no automatic software memorisation
- optional backups only offline, on physical media
- full responsibility assumed by the organisation

ARCAN protects data.
It does not protect against imprudence.

5. ARCAN within a global security architecture

ARCAN is not a standalone fortress.
It is a component within a broader strategy.

ARIEL-IA recommends integrating it into an architecture that includes:

- clear internal policies
- data segmentation
- access management
- environment separation
- organisational discipline

Digital sovereignty never relies on a single tool,
but on the coherence of the whole.

---

6. What ARCAN deliberately does not do

To avoid any ambiguity, ARCAN deliberately provides no:

- password recovery
- cloud storage
- fallback mechanism
- backdoor
- blind automation
- invisible or implicit security

These absences are not shortcomings.
They are **design choices**.

Conclusion

ARIEL-IA does not sell security.
We transmit:

- sober tools

- responsible practices
- a demanding vision of digital sovereignty

ARCAN is intended for organisations willing to accept:

- rigour
- discipline
- and the responsibility that real data protection entails

Sovereignty is never free.
It is earned through coherent choices.

✔ **Document status**
This document constitutes an official ARCAN doctrinal reference.
All development, offerings, interfaces and collaborations align with it.