CERT Abicom

RFC 2350
1.0 - 09/09/2025

abicom

10 allée Pierre de Fermat

63170 Aubière – France

Tél. 04 73 37 01 69

www.abicom.fr

Siret : 381 589 886 00039 - APE 6311Z

TLP:CLEAR

Document details

Version	1.0
Date of latest version	09/09/2025
Created by	Adrien ROUX
Approved by	Florent GROSSO
Confidentiality level	Public

This document is valid until superseded by a later version.

Version	Publication date	Object	Author
0.1	20/03/2025	Initial version	ARO
0.2	02/04/2025	Overhaul of Service section based on FIRST Service Framework	ARO
0.3	27/08/2025	Added PGP and CERT website page information	ARO
1.0	09/09/2025	Review for publishing	FGR

ABICOM 10 allée Pierre de FERMAT, Parc Technologique La Pardieu, 63 170 Aubière

Summary

1. Document information

This document contains a description of the CERT ABICOM in accordance with RFC 2350 specification. It contains basic information about the CERT ABICOM, the services offered and their scope.

1.1 Date of Last Update

This is version 1.0, published on 7 March 2024.

1.2 Distribution List for Notifications

Changes to this document are notified to CERT ABICOM constituency through closed channel.

1.3 Locations where this Document May Be Found

The current and latest version of this document can be found on Abicom's website at:

https://www.abicom.fr/cert/

1.4 Authenticating this Document

This document has been signed with the PGP key of the CERT ABICOM. The PGP public key, ID and fingerprint are available on Abicom's website at:

https://www.abicom.fr/cert/

1.5 Document Identification

Refer to document details table

2. Contact information

2.1 Name of the Team

Computer Security Incident Response Team of Abicom names:

Long name: CERT ABICOM

Short name: ABI-CERT

2.2 Address

Abicom

10 allée Pierre de Fermat,

63170, Aubière

FRANCE

2.3 Time Zone

CET/CEST

2.4 Telephone Number

CERT ABICOM main number available on French office hours:

+33 4 73 37 01 69

2.5 Facsimile Number

Not available.

2.6 Other Telecommunication

CERT ABICOM does not provide any other telecommunication channel outside its constituency.

2.7 Electronic Mail Address

CERT ABICOM team can be contacted for any inquiry related to its constituency and services by email: CERT[at]abicom[dot]fr

2.8 Public Keys and Encryption Information

Abicom CERT supports PGP/GnuPG for secure communication:

- Fingerprint: B7A1 1937 7C27 E1AF 3C42 EABB DA80 D546 B536 136F

The public key is shared with CERT ABICOM constituency. It can be retrieved from one of the usual public key servers.

2.9 Team Members

The identities of the members of the CERT ABICOM team are not publicly available. They may be disclosed on a case-by-case basis on the grounds of need-to-know restrictions.

2.10 Other Information

General information about Abicom and the services provided by the company can be found on Abicom's website: https://www.abicom.fr

2.11 Points of Customer Contact

The preferred method to contact the CERT ABICOM is via e-mail at CERT[at]abicom[dot]fr.

Please use our public key to ensure confidentiality and integrity.

Urgent assistance needs may be reported by phone (Cf. §2.4 - Telephone Number).

3. Charter

3.1 Mission statement

The CERT ABICOM is a private Computer Security Incident Response Team. Its mission is to support its constituency community with reactive and proactive services in the field of Cyber Security by:

- Gathering, evaluating, and disclosing information on vulnerabilities and threats to relevant teams for detection and vulnerability management
- Providing technical expertise on security-focused questions
- Coordinating discussions with external entities about threat intelligence and information sharing

3.2 Constituency

The primary constituency is composed of Abicom's customers with a Service Level Agreement support contract.

3.3 Sponsorship and/or Affiliation

The CERT ABICOM is part of Abicom, a company part of OCI Group (https://www.oci.fr/).

3.4 Authority

The CERT ABICOM operates with an advisory role with its customers. Any recommendation which CERT Abicom may provide will be implemented under the direction of the customer.

4. Policies

4.1 Types of Incidents and Level of Support

CERT ABICOM addresses all types of information security incidents which occur in its constituency. The level of support given by the CERT ABICOM will vary depending on the size and severity of the incident, the type of constituent, the available CERT ABICOM resources and the level of support requested by the constituent. Resources will be assigned according to the following priorities, listed in decreasing order:

- Incident response and assistance
- Incident analysis and forensics
- Malware analysis
- Alerts and advisories
- Threat intelligence analysis

Additionally, the CERT ABICOM can call upon other business units within Abicom to assist the constituents.

4.2 Co-operation, Interaction and Disclosure of Information

CERT Abicom operates under the restrictions imposed by French laws.

All information exchanged with a customer during an incident (and after its resolution) will be handled confidentially in secure environments using encryption if necessary. CERT Abicom uses the Traffic Light Protocol (TLP) and Permissible Action Protocol (PAP).

CERT Abicom will cooperate with other Organizations in the field of Computer Security, which may help to deliver its services, especially for incident resolution. In any such exchange, CERT Abicom will protect the privacy of its customers through anonymization of technical data which may be exchanged. Customers will be informed of such exchanges.

If a customer objects to the default behavior of CERT Abicom, it should be specified in an initial contractual agreement or explicitly asked for in the communications with CERT Abicom. Requiring specific behavior may lower the quality of assistance CERT Abicom may provide.

4.3 Communication and Authentication

The CERT ABICOM ‘s preferred contact method is e-mail. For the exchange of sensitive material, please use the PGP key specified in section 2.8 to encrypt data. The CERT ABICOM may also use other encryption methods on a case-by-case basis, for example when regulation requires specific encryption technologies.

5. Services

The services provided by the CERT Abicom follow the services described by the FIRST Services Framework.

5.1 Information Security Incident Management

CERT Abicom provides comprehensive support for managing cybersecurity incidents, from initial reporting to resolution, including coordination with stakeholders and authorities where necessary.

5.1.1 Information Security Incident Report Acceptance

CERT Abicom accepts reports of suspected or confirmed security incidents from its constituency ensuring secure and timely intake through defined communication channels provided to its constituency. Assistance will be provided during business hours by default, but any constituent can ask for assistance on a 24/7 basis if necessary. Reports are triaged based on severity, impact, and urgency.

5.1.2 Information Security Incident Analysis

CERT Abicom conducts detailed technical and contextual analysis for incidents. This includes verifying if the activity is legitimate or malicious, and for the later identifying indicators of compromise (IoCs), identifying attack vectors, assessing impact, determining affected assets or services, and classifying the incident type and severity for its constituency.

- Analysis methods include log reviews, network traffic inspection, endpoint telemetry analysis, and threat intelligence correlation.
- Findings are documented and shared with relevant stakeholders within the constituency to provide appropriate responses.

5.1.3 Artifacts and Forensic Evidence Analysis

CERT Abicom analyzes digital artifacts (such as malware samples, logs, emails, and forensic images) related to incidents reported by its constituency. Forensic investigations aim to determine root cause, attack vectors, and the extent of compromise while preserving evidence integrity following recognized chain-of-custody practices.

- Capabilities include basic malware analysis (static and dynamic), indicator extraction, and forensic timeline reconstruction.

5.1.4 Mitigation and Recovery

CERT Abicom assists constituency members in implementing containment, mitigation, and recovery measures. Guidance is tailored based on the incident type, criticality of affected assets, and overall business impact.

- Support may include patching advice, system isolation procedures, malicious code eradication, configuration changes, and restoring from trusted backups.
- CERT Abicom prioritizes actions to minimize operational disruption and reduce the risk of recurrence.
- CERT Abicom assists its constituency throughout the incident resolution process, including containment, eradication of threats, system recovery, and post-incident improvement to the security posture.
- CERT Abicom also works with other Abicom business units for Audit activities (notably post-compromise security audit), Infrastructure IT teams for assistance with information system operations.

5.1.5 Information Security Incident Coordination

CERT Abicom facilitates coordination among affected parties within its constituency, as well as with external stakeholders (e.g., other CERTs, vendors, regulators) when necessary.

- CERT Abicom helps managing information flow, supports joint decision-making, and helps align technical and communication efforts during multi-party incidents.

5.1.6 Crisis Management Support

In cases of large-scale incidents or crises affecting critical services within the constituency, CERT Abicom supports executive and crisis management teams. Services include providing situational updates, technical assessments, impact forecasts, strategic advice, and assistance with stakeholder communications.

- CERT Abicom helps activate crisis management structures, assist in the incident response coordination, and contributes to post-crisis lessons learned activities.

5.2 Information Security Event Management

CERT Abicom's SOC Team manages and analyzes cybersecurity events relevant to its constituency with the appropriate contract to detect threats early, contain emerging risks, and improve overall resilience. Event management activities focus on early identification and triage of suspicious activities among routine operational noise.

5.2.1 Monitoring and Detection

CERT Abicom monitors security telemetry provided by or relevant to its constituency. Sources can include Endpoint Detection & Response tools, SIEM platforms, IDS/IPS systems, cloud services, and external threat intelligence feeds. Analysts evaluate the telemetry to ensure proper identification of legitimate events versus potentially malicious activity.

5.2.2 Event Analysis

CERT Abicom analyzes observed security events to determine their significance, potential impact, and need for escalation. Significant events can be escalated to full incident status and handled by the incident response team.

- Event analysis involves correlation with known threats, contextual enrichment, and impact estimation tailored to the affected members of the constituency.
- Where appropriate, early warnings are issued to relevant constituents to promote rapid response.

6. Incident reporting forms

No specific incident reporting form must be completed. Incident key points will be determined during the qualification phase following the qualification process in place in the CERT ABICOM team

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, the CERT ABICOM assumes no responsibility for errors or omissions, or for damage resulting from the use of the information contained within.