1. Document information

This document contains a description of CSIRT NOMIOS in accordance with RFC 2350 specification (ietf.org/rfc/rfc2350.txt). It provides basic information about CSIRT, and describes its responsibilities and services offered.

Date of last update	Version 1.2, published on 2023-12-09.
Distribution list for notifications	N/A
Locations where this document may be found	The current and latest version of this document is available on demand or on the NOMIOS CSIRT webpage.
Authenticating this document	We can provide a signed version of this document with the PGP key of the CSIRT.
Document identification	• **Title:** RFC 2350 - Information regarding the NOMIOS Group CSIRT • **Expiration:** This document is valid until superseded by a later version.

2. Contact information

Name of the team	**Official name:** CSIRT NOMIOS **Short name:** CSIRT NOMIOS
Address	[headquarters] 64 av. Jean-Baptiste Clément - 92100 Boulogne-Billancourt - FRANCE
Time zone	UTC+1 (Europe/France/Paris)
Telephone number	+33 (0)1 41 10 28 48 (NOMIOS FR – Support)
Facsimile number	Not applicable.
Other telecommunication	Custom and secure transfer method during investigation.
Electronic mail address	If you need to notify us about an information security incident, please contact us at: [csirt@nomios.fr].
Public keys and encryption information	Download link: https://keys.openpgp.org/vks/v1/by-fingerprint/8C5BB36D8D1380F2D3CD7FD051A98DCFDF92B36A Fingerprint: **8C5B B36D 8D13 80F2 D3CD 7FD0 51A9 8DCF DF92 B36A** -----BEGIN PGP PUBLIC KEY BLOCK----- mDMEaXD5rRYJKwYBBAHaRw8BAQdA1ryoV+x/vzgzzHW3ebYJNOd8n+oUEzAeqt1t Uz13bJe0HkNTSVJUIE5PTUlPUyA8Y3NpcnRAbm9taW9zLmZyPoi1BBMWCgBdFiEE jFuzbY0TgPLTzX/QUamNz9+Ss2oFAmlw+a0bFIAAAAAABAAObWFudTlsMi41KzEu MTEsMiwxAhsDBQkFpKQDBQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheAAAoJEFGp jc/fkrNqWBwBALw3ZKyZY14Wofg0dZMDQ6Vn27fGQhcVbHCfBSQp1jFYAP9+UZJg xf00biN9VXXHb/gMA/PJpxl1Bn+ghMafI7lmD7g4BGlw+a0SCisGAQQBl1UBBQEB B0B06NATAxjjyXHd43y8RSpi66psrRhSDdT1nu4c5HMjPgMBCAeImgQYFgoAQhYh BIxbs22NE4Dy081/0FGpjc/fkrNqBQJpcPmtGxSAAAAAAAQADm1hbnUyLDIuNSsx LjExLDIsMQIbDAUJBaSkAwAKCRBRqY3P35KzanTWAQCzWwgErOhowAnQUWsntkId CfNr+VjmUIoMZilm0yDRZAD8CXkAOiCp8jCLugLFpc8rnPYWUzDD4p+T0LBRlcN/ IAc= =f5lX -----END PGP PUBLIC KEY BLOCK-----

Team members	Team members are not publicly listed.
Other information	N/A
Points of customer contact	CSIRT NOMIOS prefers to receive incident reports via the Nomios website (https://www.nomios.fr/contact/), the support portal (https://support.nomios.fr/) or by email (csirt@nomios.fr). CSIRT NOMIOS hours of operation are 24/7 or depending on the subscribed offer.

3. Charter

Mission statement	Incident response and other incident management services
Constituency	• **Primary constituency:** Clients who have subscribed to the "Managed CSIRT" service offer. • **Secondary constituency:** Partner CSIRTs/CERTs and legal or regulatory authorities.
Affiliation	Nomios Group
Authority	The CSIRT NOMIOS acts as an outsourced technical incident response resource for our clients. The authority to execute actions (e.g., system disconnection) remains the contractual and legal responsibility of the client. We act based on a mandate and a formalized agreement (SLA/service contract).

4. Policies

Co-operation, interaction and disclosure of information	CSIRT NOMIOS cooperates with other CERTs and law enforcement agencies, always respecting client confidentiality agreements and applicable laws. All client data is treated as **confidential and sensitive**. We use the **TLP** (Traffic Light Protocol) for information exchange with third parties.
Communication and authentication	The preferred method of communication is via the support portal or email. For the exchange of sensitive information, CSIRT NOMIOS uses PGP for encrypting and/or signing messages.

5. Services

Incident response	CSIRT NOMIOS provides incident response services including post-mortem analysis (DFIR reports) and strategic recommendations.
Incident triage	Identification of the scope, attack vector, and Indicators of Compromise (IOC).
Incident coordination	Crisis Management and Executive Support
Incident resolution	Assistance with containment (isolation of infected systems), eradication (cleaning up malware), and restoration return to normal operations.
Proactive activities	Proactive threat hunting.
Vulnerability management	DTM and Nomios VOC service
Cyber threat analysis	Cyber watch (Threat Intelligence) and distribution of targeted client alerts.

6. Incident reporting forms

- The preferred methods for reporting incidents are:
  - Nomios website: https://www.nomios.fr/contact/
  - Support portal: https://support.nomios.fr/
  - Emergency e-mail csirt@nomios.fr (PGP encrypted if possible)
- Required information:
  - Date and time of discovery, nature of the incident, impact, technical contact details.

7. Disclaimers

- **Service conditions (SLA):** Details regarding response times, availability, and costs are found in the Service Level Agreement (SLA) attached to the contract.
- **Exclusions of liability:** CSIRT NOMIOS is not responsible for damage occurring before or after its intervention, or damage resulting from the non-respect of recommendations by the client.
- **Jurisdiction:** French jurisdiction and laws.

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