Security requirements for consuming NaC APIs

Last updated 15 April 2026

Purpose

This document outlines mandatory security requirements for all customers consuming NaC APIs.

Scope

These requirements apply to the customer IT environment including cloud service providers, devices and third-party services used to access NaC APIs and related data. Customers must ensure that cloud or third-party providers commit to enforcing all relevant NaC and privacy security requirements in order to protect NaC API's response data.

Requirements

Security Governance

- Customers must implement security measures aligned with industry best practices (e.g. ISO 27001, ISO22301), applicable laws, and ensure subcontractor compliance. The Customer also agrees not to communicate to third parties any information that may pose a danger to the confidentiality, security or integrity of Nokia's Platform or API provider's information, or which may impair Nokia or API provider's privacy or intellectual property rights.
- Customers must operate a risk-management process covering critical assets, threats, proactive controls and documented risk management plans.

Network and Infrastructure Security

- All in-scope devices and applications must be protected by a properly configured firewall or equivalent control.
- Default administrative password of All in-scope devices and applications must be changed or remote administrative access disabled.
- The Customer must prevent access to the administrative interface for in-scope devices and applications from the Internet, unless there is a clear and documented business justification and the interface is protected by Multi-Factor Authentication and IP whitelist.
- The Customer must block unauthenticated inbound connections by default for IT infrastructure in scope.
- The Customer must implement a malware protection mechanism on IT infrastructure in scope.
- The Customer must keep anti-malware software and all associated malware signature files up to date, with signature files updated at least daily. This may be achieved through automated updates, or with a centrally managed deployment. Also, there are additional requirements for the use of anti-malware software:
    - The Anti-malware software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.

    - The Anti-malware software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).
    - The Anti-malware software must provide web-filtering capabilities and traffic analysis.
-

Configuration Change Management

- All infrastructure changes must be authorized, documented and linked to a valid business requirement.
- The Customer must ensure an adequate segregation of duties that allow effective control and adequate access restriction in the execution of critical tasks.
- Unnecessary configurations and software must be removed or disabled, with periodic review to ensure minimal attack surface.
- The Customer must turn off any auto-run feature that executes files without approval (such as those downloaded automatically from the Internet).

Integrity Protection

- The Customer must implement authentication methods, such as digital signatures, to maintain integrity of code and information throughout the system's life cycle.
- The customer must implement robust cryptographic algorithms for encryption of all frontend application and backend application server communication.
- Customers must maintain encryption of data both in transit and at rest by employing cryptographic algorithms that adhere to industry’s best practices.

Access Management requirement

- Customers are responsible for managing all user accounts, including those of third parties, as well as overseeing access privileges.
- Customers must implement strong access-management practices aligned with industry good practices. The Customer must implement:
    - Formal process for account creation and approval
    - Robust authentication control
    - MFA required for all cloud services
    - Unique user accounts required for administrative tasks
    - Enforce least privileged access
    - Conduct periodic access reviews (at least annually) and removal of unneeded privileged access

Password & Authentication Controls

- Password quality must be ensured via one of the following:
    - A minimum password length of at least 12 characters.
    - A minimum password length of at least 8 characters and use deny list for common passwords.

- Customers must implement device locking controls. Devices requiring physical access (e.g., laptops, mobile phones) must be unlocked with a credential—such as biometrics, password, or minimum 6 characters PIN—before services can be accessed.
- Brute-force protection must limit attempts (max 5 attempts within 10 minutes or enforced lockout).
- The Customer must require regular password changes and prevent reuse of the last five passwords.
- Compromised credentials must be changed immediately.
- API keys or credentials used for accessing NaC APIs or NaC platform must be stored securely (e.g., in a secure vault). Compromised or suspected-compromise keys must be revoked and replaced without delay.

Secure development

- The customer must maintain a risk-based secure development policy to protect personal data sent through NaC APIs. The policy should include, at least, the following areas:
    - Secure software design for apps and APIs should follow the principle of minimum necessary information.
    - Development source code should not be stored on production systems.
    - Changes to code must follow version control in accordance with good industry practices and maintain audit trails.
    - Testing with production API response data that includes actual mobile subscribers is strictly prohibited unless expressly authorized by Nokia or the API provider. All proofs of concept should utilize test data from pre-production environments whenever feasible and must always be conducted within a controlled setting (such as user/customer/data whitelists approved for the pilot).
- Customers must follow industry best practices (like OWASP Guide, SANS CWE Top 25, SAFEcode, CERT Secure Coding) when developing software applications. At a minimum, they should use sandbox systems, avoid insecure string/storage functions, validate inputs/outputs, use precise integer operations for memory and arrays, choose libraries to prevent cross-site scripting, use canonical formats, avoid string concatenation in dynamic SQL, eliminate weak cryptography, implement logging and tracing.

Vulnerability and Patch Management

- The customer must perform Security testing after each major software changes and at least annually.
- The Customer must follow the industry's best practices for software vulnerability management.
- The Customer must implement management process for the installation of periodic patches through change management that ensures the treatment of known vulnerabilities and that they comply with security standards or regulations.

- The Customer must deploy the necessary patches on high-risk systems as urgently as possible. In case of vulnerabilities in production that may expose risk to NaC APIs and associated data, these must be corrected in a commercially reasonable timeframe. Nokia reserves the right to block the APIs in case of detection.

Privacy Management

- The customer guarantees that it carries out adequate management of personal data and appointment of a Data Protection Officer if applicable, following the terms established in applicable local regulation or law, and the agreed DPA.
- The Customer must securely delete NaC's API associated data with the service when it is no longer strictly necessary based on the service agreement with Nokia or applicable law, or in the event of termination of the contract.
- The data delivered by the exposed API must always be protected at all levels of the chain.
- User's IP addresses and privacy sensitive information shall not be shared with third parties without the user's consent.

Audit and Accounting requirements

- The customer must maintain a team responsible for performing audit activities on its systems or procedures, independently of the areas being audited, in accordance with applicable laws or regulations.
- The customer must have adequate management and technical controls for the retention of security logs that guarantee the custody and integrity of the access records of operators and administrators to the systems and applications that are the object of the service, and especially those that process personal data.

Security and Privacy incident reporting

- Any identified privacy or API related risk must be reported to Nokia immediately without undue delay.
- The Customer must report, without undue delay, any significant security incident or privacy data breach incident, own or that its third parties that may cause operational disruption or loss as well as those that may cause material or immaterial damage to natural and legal people of NaC APIs, API providers behind NaC platform and their end customers.
    - Such communication to Nokia will be made to security.networkascode@nokia.com as soon as possible and, in any case, within a maximum period of 48 hours from the date of becoming aware, by means of an early warning with as much information as possible, and within 72 hours an updated notification of the incident must be made with an initial assessment of the same, including severity and impact and commitment to resolution if possible, in which case, both companies will remain in constant contact until resolution. Within a maximum period of 1 month from the notification, a final report will be sent containing a detailed description of the incident, severity and impact, type of threat or main cause of the incident, measures implemented and underway, and the repercussions of the same. Nokia can inform

the competent authorities and external stakeholders as per legal requirements as applicable.

Security Training

- The Customer must conduct annual security awareness training that must cover security requirements in this document. The Customer will inform its workers, subcontractors and third parties of the safety measures in place to ensure that its employees comply with the codes of good security practice established in the industry and NaC security requirements.