Cloud Services Policy

Introduction

The entrustment of data in the cloud pursuant to EN ISO/IEC 27017:2021 involves the verification of certain requirements for both the Customer and NIDEK Technologies.

NIDEK Technologies, in complete transparency for the management of the services offered, then provides a summary of the obligations referred to the Customer and those adopted by NIDEK Technologies as a supplier in compliance with EN ISO/IEC 27001:2023, EN ISO/IEC 27017:2021 and EN ISO/IEC 27018:2020.

If the Customer finds any discrepancies with respect to what is reported below and any services offered, he is invited to report it by sending an email to service@nidektechnologies.it.

Applicability

This policy applies to cloud services managed by NIDEK Technologies.
This policy does not apply when NIDEK Technologies services run on cloud systems managed directly by the Customer.

References

Latest applicable versions of ISO 27001, ISO 27002, ISO 27017, ISO 27018.
General Data Protection Regulation (GDPR) (EU) 2016/ 679.

Glossary

Information security event: occurrence indicating a possible information security breach or failure of controls.

NIDEK Technologies Cloud Infrastructure: The virtualized infrastructure composed of computing instances, database instances, storage systems, services, and applications deployed in the cloud. It forms the foundation for delivering NIDEK Technologies Cloud Services.

N**IDEK Technologies Cloud Network**: A collection of communication protocols and physical or cloud-based network resources that interconnect the components of the NIDEK Technologies Cloud Infrastructure.

NIDEK Technologies Cloud Services: A suite of services delivered by NIDEK Technologies to its customers through the NIDEK Technologies Cloud Infrastructure.

PROCEDURES

Cloud services protocol

The data stored in the cloud computing environment may be subject to access and management by NIDEK Technologies; to protect the Customer, NIDEK Technologies adopts methods and processes certified by third parties in the fields of EN ISO/IEC 27001:2023, EN ISO/IEC 27017:2021 and EN/ISO IEC 27018:2020.

1. NIDEK Technologies has identified the Data Protection Authorities, the Italian National Cybersecurity Agency and the Postal Police as the relevant authorities for data protection. If the Customer decides to modify and/or integrate these bodies, it is required to define these aspects in advance, in a specific agreement between the parties.

2. NIDEK Technologies delivers its cloud services utilizing infrastructure provided by Microsoft through the Microsoft Azure platform (https://azure.microsoft.com/), with data hosting primarily located within the European Union or in a jurisdiction geographically proximate to the Customer's location. Notwithstanding the foregoing, upon the Customer's explicit written request, such services may be hosted in alternative geographical regions and/or on infrastructure provided by third-party cloud service providers.

3. Microsoft Azure supports one of the most comprehensive portfolios of security standards and compliance certifications in the industry, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171. Azure is also certified under ISO/IEC 27001:2022, ISO/IEC 27017:2015, and ISO/IEC 27018:2019, helping customers meet compliance requirements worldwide.

4. NIDEK Technologies shall provide the Customer with no less than thirty (30) days' prior written notice of any change in the cloud service providers utilized. Where the Customer is located within the European Union, NIDEK Technologies guarantees that the infrastructure supporting the cloud services shall remain within the European Union, unless the Customer explicitly requests otherwise in writing. Furthermore, NIDEK Technologies warrants that all data processing activities shall be carried out in compliance with the General Data Protection Regulation (Regulation (EU) 2016/679).

5. NIDEK Technologies classifies all the information exchanged with the Customer. Labelling follows the following classification levels:

Category of Information	Description	Examples
Public or unlabeled	The information provided is not confidential and therefore can be public without it having any negative implications if it is detected. The lack of availability of	Leaflets, brochures, press releases, websites, newsletters

PROCEDURES

	this information in the event of downtime is an acceptable risk. Integrity is important but not fundamental and vital to the life or business of the Customer.	
Confidential	Confidential documentation for internal or external use that contains sensitive information that should only be accessed by a small group of authorized persons, as its unauthorized disclosure could cause significant harm to the organization. This category includes information received from the Customer.	Customer contracts, offers, product development projects, internal legal documents, confidential financial information
Strictly Confidential	Documentation that contains extremely sensitive information that, if disclosed, could cause serious harm to the organization, its Customers, or its partners. Access to this information is limited to a very small number of people, with strict protection measures.	Software source codes, know-how used to process Customer information, information on patents in the process of filing, sensitive health data, cryptographic keys or security certificates

6. NIDEK Technologies' periodic asset inventory includes associated information and assets, including those stored in NIDEK Technologies' cloud infrastructure. Inventory logs indicate where assets are kept.

7. NIDEK Technologies adopts an appropriate allocation of information security roles and responsibilities and confirms that it is in a position to fulfill its data security roles and responsibilities. To this end, periodic reassessments of risk analysis, vulnerability assessments and penetration tests are conducted. In this regard, NIDEK Technologies implements its own policy for the prevention and management of threats, on which, at the Customer's request, it can provide documentation in this regard.

8. All access to the systems, services and applications on the NIDEK Technologies Cloud Infrastructure are safe and secure. To ensure high levels of protection and block any malicious access attempts, two-factor authentication (MFA) is enabled on all NIDEK Technologies Cloud Services as far as possible.

PROCEDURES

9. The management of the cloud service offered to the Customer considers the access profile to the service provided by NIDEK Technologies. NIDEK Technologies informs the Customer of the standard access methods at the time of service activation.

10. NIDEK Technologies' access control policy for its Cloud Infrastructure incorporates compartmentalization for each service.

11. NIDEK Technologies adopts a network segregation policy to achieve segregation of Customers' cloud environments. In details, NIDEK Technologies Cloud Infrastructure guarantees:
    a. segregation of groups of information services, users, and information systems, dividing them into separate Azure subscriptions.
    b. logical segregation of cloud service customer data, virtualized applications, operating systems, storage, and networks to ensure data integrity and confidentiality.

12. The Customer must ensure that the service delivery capacity agreed with NIDEK Technologies is met. NIDEK Technologies provides the Customer with the necessary tools to monitor service usage and anticipate capacity needs, ensuring optimal performance of the required cloud services over time.

13. The services provided on the NIDEK Technologies Cloud Infrastructure implement encryption controls that comply with recognized and approved security standards. In this regard NIDEK Technologies implements practices for controlling and maintaining the effectiveness of cryptographic keys throughout the application lifecycle of the , including generation, installation, updating, revocation and destruction. As a standard practice, NIDEK Technologies applies cryptographic controls to all transactions managed by the application to and from the Customer.

14. Access credentials for the application services provided by NIDEK Technologies Cloud Infrastructure are unique to each user and cannot be shared. Credentials should not be stored on written media in a manner that could facilitate unauthorized access by third parties.

15. For the application services provided by NIDEK Technologies Cloud Infrastructure, NIDEK Technologies may offer a backup service as stipulated in the contract with the Customer.

16. All activities related to addressing security issues and enhancing the usability of the services provided by NIDEK Technologies Cloud Infrastructure are conducted by NIDEK Technologies personnel with the appropriate permissions and delegations.

17. The Customer must determine the information security requirements and then assess whether the services offered by NIDEK Technologies meet those requirements. To this

PROCEDURES

end, the Customer is entitled to request information from NIDEK Technologies on the information security features adopted.

18. NIDEK Technologies conducts development operations in a secure, dedicated environment using non-production test data. These operations are governed by specific written procedures. NIDEK Technologies can provide documentation on this process at the explicit request of the Customer.

19. The Customer must include NIDEK Technologies in its information security policy, in its relations with suppliers. This will help mitigate the risks associated with accessing and managing the data hosted in the services offered by NIDEK Technologies.

20. The Customer must confirm the roles and responsibilities regarding the security of information relating to the services provided by NIDEK Technologies and described in the relevant contract.

21. NIDEK Technologies has a specific written procedure for handling information security incidents. This policy ensures a consistent and effective approach to addressing such incidents, including communications related to security events.

    The policy aims to mitigate the following risks:

    1. Reduce the impact of information security breaches by ensuring that incidents are properly followed.
    2. Identify areas for improvement to reduce the risk and impact of future incidents, decreasing the attack surface and the chances of Data Breaches.

    Information security incidents should be reported as soon as possible by sending an email to service@nidektechnologies.it. Upon verification of the incident, the responsible staff will evaluate the situation and implement appropriate corrective actions and/or containment measures.
    In the event of a data breach, it should be reported to the NIDEK Technologies service department (service@nidektechnologies.it), who will activate NIDEK Technologies' specific operating procedure for managing data breaches. This includes promptly notifying the Personal Data Protection Authority and the Customer's project leads about the breach.
    A "Security Incident Report" will be created for Information Security Incidents.
    An "Information Security Incident" is an event that has caused or has the potential to cause damage to NIDEK Technologies' assets, reputation and/or customers. Such incidents include but are not limited to:

    a. The loss or theft of data or information (Data Loss).
    b. The transfer of data or information to those who do not have the right to receive that information (Data Leakege).

PROCEDURES

c. Attempts (failed or successful) to gain unauthorized access to the data or information files (DataStore) of a computer system of NIDEK Technologies or its Customers.
d. Fraudulent changes to information or data in a computer system.
e. Unsolicited disruption of a service provided by NIDEK Technologies Cloud Infrastructure.
f. The action of malware or a DDOS attack.

The Customer must provide the following essential information:

g. If the loss of data puts any person or other data at risk.
h. The date and time the security incident occurred.

It is therefore essential that the Customer identifies any weakness related to the security of information that has been observed or suspected in the services provided by NIDEK Technologies.

NIDEK Technologies will respond to information security incidents in accordance with documented procedures. The knowledge gained from the analysis and resolution of information security incidents will be used by NIDEK Technologies to reduce the likelihood or impact of future incidents.

22. All data in transit managed on the NIDEK Technologies Cloud Infrastructure is encrypted using secure encryption protocols such as TLS.

23. In the event of severe force, natural disasters, terrorist acts or any other catastrophic events that are reasonably unforeseeable and impact the infrastructure underlying NIDEK Technologies Cloud Infrastructure, NIDEK Technologies reserves the right to migrate the services provided to the Customer to another ISO 27001, ISO 27017, and ISO 27018 certified provider, provided that the Disaster Recovery service is included in the contract with the Customer.

24. The data processed by the Customer as Data Controller on the NIDEK Technologies Cloud Infrastructure will always be controlled by the Customer.

25. NIDEK Technologies, in compliance with EU Regulation 2016/679 (GDPR), guarantees the data controller the possibility of receiving at any time a copy of the data in a structured, commonly used and machine-readable format ("right to access"), as well as knowing the physical location where the data resides.

PROCEDURES

26. NIDEK Technologies ensures data and application portability, if the Customer opts to migrate to another cloud provider, thus preventing vendor lock-in.

27. NIDEK Technologies, in compliance with EU Regulation 2016/679 (GDPR), guarantees the data controller the deletion of his or her data ("right to be forgotten").
The right to erasure takes precedence over the interest in data retention. In such cases, if a data controller requests the deletion of their data, NIDEK Technologies will proceed without undue delay and will not reserve the right to continue processing the data until the originally set deadline, regardless of whether that deadline is imminent or not.

28. NIDEK Technologies, as personal data cloud processor, commits to including a provision in its contracts with customers that requires notification of any legally binding requests for the disclosure of personal data by law enforcement authorities. NIDEK Technologies will provide such notifications in accordance with the agreed-upon procedures and timeframes established in the contract, unless prohibited by the law enforcement authority from disclosing such information. This ensures that customers are informed and can take appropriate action regarding any requests for personal data disclosure.

29. NIDEK Technologies has a specific policy in respect of the return, transfer and/or disposal of personal data. In the event of an explicit request by the Customer, NIDEK Technologies is available to provide this document.

30. It is the Customer's responsibility to request a documented description of the process of terminating the cloud service provided by NIDEK Technologies covering the removal of the Customer's assets followed by the deletion of all copies of such assets from NIDEK Technologies' systems. To this end, NIDEK Technologies will provide specific plans for decommissioning a service, including how to return data (where necessary).

31. NIDEK Technologies is committed to ensuring that all information, concepts, ideas, procedures, methods, and technical data that its staff become aware of while providing services to the Customer are treated as confidential and subject to secrecy.
NIDEK Technologies takes all necessary precautions with its collaborators to protect the confidentiality of such information and documentation. Additionally, NIDEK Technologies adheres to personal data processing legislation and respects the rights of individuals and other entities in accordance with the Italian Personal Data Protection Code (Legislative Decree 196/03 and subsequent amendments) and Regulation 2016/679 and its applications.

    If the Customer deems it appropriate to request documented evidence of the implementation of specific security controls related to the services provided by NIDEK Technologies, and if this does not pose a risk to the information security of NIDEK Technologies and/or its Customers, such documents will be classified as 'Confidential' and provided to the Customer.

PROCEDURES

32. NIDEK Technologies implements hardening as a process to enhance the security of cloud environments used for providing services to customers. Two approaches are followed:

    a. One Time Hardening. it is carried out only once and after the first setup of the environment;

    b. Multiple time hardening. it is carried out several times during the life of the environment, depending on major upgrades of the operating system or installation of additional modules/libraries

33. NIDEK Technologies ensures that once the Customer's cloud environment is deallocated, the deletion of all data is requested without delay to the service provider. This process guarantees that no residual data remains.

34. All communications to and from NIDEK Technologies' Cloud Service are transmitted securely using HTTPS, SSL, and TLS protocols, ensuring that data reaches its intended destination without being disclosed.

35. NIDEK Technologies ensures the limited use of printed materials, which are destroyed by shredding when they are no longer needed.

36. NIDEK Technologies ensures that copies of security policies and operating procedures are maintained for a period of at least 5 years.

37. The Customer should consider that applicable laws and regulations may include those governing both NIDEK Technologies' jurisdiction and its activities.