

---

# Digital Insurance Policy Guidelines, 2024 (2081)

---

Date of Approval: 2081/01/07



DIGITAL INSURANCE POLICY GUIDELINE, 2024 (2081)

KUPANDOL, LALITPUR

Phone Number: +977-1-5421079, 5428604, 5438743

## Digital Insurance Policy Guidelines, 2024 (2081)

**Preamble:** Whereas it is expedient to utilize digital platforms for facilitating swift, transparent and organized sales, distribution, and claim settlement of insurance products and services while ensuring consistency in the operational procedures of insurance companies, the Nepal Insurance Authority has issued the following guidelines pursuant to the authority vested by Section 166 of the Insurance Act, 2022 (2079BS).

### Chapter-I Preliminary

1. **Short Title and Commencement:** (1) These guidelines shall be cited as “Digital Insurance Policy Guidelines, 2024 (2081).”

(2) These Guideline shall come into force from Mid-July, 2024

2. **Definition:** In this Guideline, unless the context otherwise requires:

- (a) “**Act**” means the Insurance Act,2022 (2079 BS).
- (b) “**Agent**” means a licensed insurance intermediary person or organization other than an employee of the insurer acting on a commission basis on behalf of an insurer.
- (c) “**Authority**” means the Nepal Insurance Authority constituted pursuant to Section 3 of the Insurance Act, 2022 (2079).
- (d) “**Certificate**” means a Digital Signature Certificate issued under Section 30 of the Electronic Transaction Act, (2008)2063.
- (e) “**Computer Database**” means an organized collection of structured information or data (i.e., data, image, voice, or audio-visual form), typically stored digitally in a computer system.
- (f) “**Digital Insurance Account**” hereafter called DIA is a digital account opened by an individual/ institution with an insurer wherein the KYC, insurance policies, and other information/documents of an individual/ institution are held in a digital form.
- (g) “**Digital Insurance policy**” means a policy document that is evidence of an insurance contract digitally signed by an insurer and issued digitally to the policyholder by the insurer.
- (h) “**Digital Record**” means the data, image, visual, or sound transmitted received, or stored in a digital form by generating the same through any means.
- (i) “**Digital Signature**” means a signature made in any digital form to be included in the transformation of a digital record by a person having a non-transformed initial digital record and the public key of signatory by using a type of asymmetric crypto system that may clearly ascertain the following matters: -

(i) whether or not the transformation of digital record was created by using a type of private key keeping a logical consistency with the public key of the signatory; and

- (ii) whether or not the initial digital record has been changed after the transformation of the digital record.
- (j) **“E-Proposal”** means a proposal form for an insurance policy filled digitally by an individual/ institution with a digital signature or e-signature or Biometric and validated by One Time Password (OTP).
- (k) **“E-Signature”** means the signature captured in the device using hand motion or stylus pen.
- (l) **“Insurance Business”** means Life Insurance Business or Nonlife Insurance Business and the word also includes Micro life, Micro non-life, and Reinsurance.
- (m) **“Insurance premium”** means an amount that an insurer collects from an insured as a return for insurance in a lump sum or installments.
- (n) **“Insured”** means a person insuring and the term also includes the person entitled to the benefit arising out of an insurance policy.
- (o) **“Insurer”** means a corporate body registered and licensed under the Act and the word also includes the micro life, Micro non-life, and Re-insurer.
- (p) **“Multi-factor authentication”** means an authentication method that requires the user to provide two or more verification factors to gain access to an insurance resource.
- (q) **“Personal information”** means any information that can be used on its own or with other information to identify, contact, or locate an individual or person.
- (r) **“Regulation”** means the Insurance Regulation, 1993 (2049 BS).

## Chapter-II

### **Digital Insurance Policy for Insurers**

3. **Creation and operation of Digital Insurance Account:** (1) Every insurer can create a Digital Insurance Account for every customer who wishes to purchase an insurance policy through a digital medium.
- (2) Upon creation of a, a username and password shall be provided to the customer and the account shall have multi-factor authentication to sign in.
- (3) After the creation of DIA, a KYC form in the format approved by the Authority shall be filled and verified by an authorized representative of the insurer proceeding with policy purchase.
- (4) The DIA number should be unique for each user with company code at the beginning restricting multiple accounts (de-duplication account) of users.
- (5) It shall be necessary for a customer to have either an email ID or a registered mobile phone number while creating DIA.
- (6) The customer shall not be charged any amount, and a single DIA number shall be issued for a single user to restrict multiple accounts of the same user.
- (7) The DIA can be created by a natural guardian or the legal guardian in case of a minor in accordance with the provisions of the Act.
- (8) The DIA can be created by a certified agent subject to the approval of the insured through OTP or email authentication.

(9) The insurer can make a necessary digital platform for agents and can also link the DIA account and E-Proposal with the agent platform as per need with proper security measures and subject to the approval of the insured through OTP or Email authentication.

(10) In-case of operation of DIA account for visually challenged, a representative nominated by him/her shall take the responsibility of the DIA holder. The representative shall make a declaration confirming the maintenance of confidentiality and communication, the status, and updates of DIA to visually challenged DIA holder.

(11) Due authentication shall be ensured each time by the insurer to ensure that services are accessed by only those authorized to access DIA.

**4. E-Proposal Form:** (1) Every insurer in order to use the digital medium shall create an E-Proposal form as per the proposal form approved by the Authority. Such a form should enable to capture the information in digital form.

(2) The E-Proposal form shall automatically capture the DIA number and its needed information. Information/data should not be asked repeatedly.

(3) When an individual furnishes the details in E-Proposal form, it shall carry his E-signature or biometric or digital signatures and if an institution fills the E-Proposal form, it shall carry E-signature of authorized staff and stamp of the institutions. The E-Proposal form upon submission shall be validated by One Time Password and email verification.

(4) E-Proposal form shall have the provision to capture details of agent if the DIA holders use the service of agents.

(5) The insurer shall make necessary arrangements to capture the information related to KYC in the E-Proposal form and a live photo or Video capture of the customer/subject matter of insurance or upload of photo.

(6) In the case of life insurers, insurers can also make a necessary digital platform to capture medical information to underwrite as per need.

(7) In the case of Nonlife insurer, E-Proposal form shall have the provision to upload photograph or video or both subject matter of insurance.

(8) For the verification of whether the E-Proposal form is filled in by the valid customer, the insurer can make use of different digital mechanisms as deemed necessary.

**5. Issuance of Digital Insurance Policies:** (1) The insurer can issue the insurance policy through online medium, subject to the Acts, Regulations, Rules and Directives, Circulars issued by the Authority and Underwriting Manual of the Insurer.

(2) An E-Proposal form shall be examined and accepted or rejected or withheld with reason by the insurer within forty-eight hours and such status shall be notified to insured.

(3) The insurer arranges e-banking or digital payment system to collect premiums. Insurers are not allowed to issue digital insurance policies without realizing premium in insurer bank accounts or valid bank guarantee as per the Act and Regulation.

(4) Digital insurance policies shall include the DIA number of policy holders.

(5) Insurer shall issue only those policies through digital medium that are listed in Annexure. If the insurer wishes to issue additional line of business through digital medium, insurer shall file prior approval as per guideline 15.

(6) Physical version of the digital insurance policies need not be issued when digital insurance policies are issued through the digital platform.

(7) The insurance policy, proposal form and other documents shall be provided with the option to print or download whenever necessary.

(8) Digital Insurance Policies shall be deemed compliant only when issued with the digital signature of the insurer in accordance with the applicable provisions prescribed by law.

(9) Insurers shall ensure confidentiality and security of insurance policies issued through digital medium.

(10) The insurer shall collect the stamp duty due for issuance of insurance policy and premium receipt and deposit the amount in bank account of Nepal Rastra Bank (NRB) or Nepal government or account prescribed by NRB to issue digital policy.

(11) The insurer shall send an electronic copy of the insurance policy via email with the phrase “This is a digitally generated and signed policy, hence bears no signature” at the end of the policy.

(12) The duly company stamped on printed form of digital policy in physical form shall be issued, if necessary, upon the request of the policy holder.

**6. Conversion of Existing Policies into Digital Form:** (1) The insurer can make the necessary arrangements to convert existing policies of DIA holder into digital form if requested by him/her; such request may be made either in digital or physical form indicating the details of policy number and DIA number.

(2) The Insurer shall display on their website necessary arrangements for conversion of existing physical policies into digital form.

**7. Digital Payments:** (1) Insurer shall make necessary arrangements for payment through digital medium, when issuing new insurance policies and renewal through DIA.

(2) Insurers must use licensed digital payment gateways or via mobile/e-banking while making or receiving payments.

(3) Digital payments made by any individual/institution other than the insured himself or proposer or policyholder or person without insurable interest shall not be acceptable.

**8. Payment of Policy Benefits:** (1) The insurer shall make necessary arrangements for providing claim, survival benefit and loan or surrender benefit through digital medium. Payment shall be made through licensed digital payment gateway or mobile or e-banking.

(2) The insurer shall make a digital claim payment system for all policies, specifically policies which are issued digitally.

(3) The insurer shall pay a certain amount of claim through digital claim payment system in specific portfolio as per company claim manual.

**Prerequisites of Information Technology, Infrastructure and Security**

9. **Operation and Use of Information Technology Systems:** The insurer shall have the necessary Information Technology infrastructure and digital policy issuance manual with digital claim settlement to issue and manage digital insurance policies.
10. **Digital Insurance Policy Issuance System:** (1) Insurers can create and use websites, mobile apps, or other types of digital medium convenient to operate and issue digital insurance policies.
- (2) The system of digital insurance policy through the website, app or other types of digital medium created and operated by the insurer must have to be updated from time to time.
11. **Minimum Requirements:** (1) The insurer's website or app or other types of digital medium, developed to issue digital policy shall have at least the following requirements: -
- (a) the user sign-in/sign-up button should be visible on the website or app or other types of digital medium.
  - (b) the procedure to purchase an insurance policy through digital medium must be clearly mentioned on the website or app or other type of digital medium.
  - (c) classification of all the insurance policies offered by the insurer through digital medium and the portfolio in which it belongs along with the benefits, terms and conditions and exclusions and of the policies.
  - (d) claim procedure, documents required and time for claim settlement as prescribed by authority for digital claim filing.
  - (e) the sitemap must be clearly visible.
  - (f) inquiry section which enables customers to post queries and get a reply from the insurer via Email, Phone, SMS, or Website.
  - (g) Frequently Asked Questions (FAQs) must be clearly visible.
- (2) When a customer signs into their DIA, the user dashboard should display the following information at a minimum: -
- (a) “Profile Section” to fill in information for the KYC form in the format prescribed by the Authority. It also includes a feature to preview the filled details.
  - (b) “Purchased Policy” section with the feature to fill the E-Proposal form in the format approved by the Authority, upload necessary documents, and make premium payments. Different policies offered by the insurer through digital medium should be available in a drop-down menu.
  - (c) “Insurance Policy” section must include digital copies of policies purchased by the customer, information on previous premium payment and premium amount due along with the next premium payment date and the status of the policies (including enforce status, Bonus status, Loan status, Nominee/Assignment Status, etc.) and a customer profile and other documents must be available.

- (d) “Policy Renew Section” providing information of issued policies on but not limited to policy renewal date, renewal premium amount, expiry/maturity date and an e-payment button must be available.
- (e) “Claim section” containing file claim button, tracking of claim status and claim related support.
- (f) “Premium calculator” for each insurance policy and for different premium payment mode along with the total premium payable under that policy.
- (g) “Help section” with help desk support for individual police and the contact number and email address of the authorized staff.
- (h) “Tracking section” to track the status of application form, payment, document upload policy status, claim application, claim status. Tracking shall be made possible via mobile number, application number or policy number with two factor authentications (e.g., Date of Birth, Citizenship number etc.)
- (i) “Mini statement” showing the basic details like name, contact details, nominee details, payment terms, sum assured, premium payable, etc. as provided in the policy schedule for each policy purchased by the customer shall be provided to the DIA holder. Full terms/conditions and exclusions may be excluded.
- (j) “settings section” must be provided for account password change and other privileges.
- (k) “FAQs” section must be present.
- (l) “Password reset option” must be available for user with authorization/identification process.

**12. Authorized Personnel for DIA:** (1) An insurer shall appoint a staff as authorized personnel who must be entitled to verify the details filled in by the DIA holder.

(2) The Authorized Personnel shall be responsible for verification of the KYC form, E-Proposal form, and documents uploaded and ensure payment of premium.

(3) The Authorized Personnel shall have an account which shall include a Verify KYC section with an approve/reject button, an Email/ SMS button to ask for additional documents, an E-Proposal form verifying section, a Policy issue section to approve and issue policies to the customer, Claim section and Logout button.

**13. KYC Details:** (1) A DIA holder must inform the Insurer about the change of KYC details, and the same shall be applicable to all policies issued to that DIA holder. The insurer shall ensure the change in the KYC through the DIA.

(2) While effecting a change of details at the request of a DIA holder, the authorized personnel of the insurer may on their own verify the change in KYC.

(3) Every change should be recorded and notified to DIA holder and provide a record of changes to the Authority when asked for.

**14. Infrastructure and Security:** (1) The insurer, before commencing the sale of insurance policies through digital mediums, shall put in place measures to safeguard the privacy of

the data and adequate systems to prevent manipulation of records and transactions. The safeguards put in place shall be reviewed on a continuous basis.

(2) The insurer shall create a subdomain of the insurer's website domain for the purpose of issuing digital policies.

(3) The insurer shall ensure the protection of the automatic data processing systems against unauthorized access, alteration, destruction, disclosure or dissemination of records and data.

(4) If the authorized persons or the servers are in multiple location, the network through which digital means of communications are established must be secure against unauthorized entry or access; for example: a VPN connection or other private secure connection.

(5) Every system firmware, software, and operating system used to issue Digital Insurance Policies shall be constantly upgraded and up to date.

(6) A virtual isolated environment or dedicated server shall be used for issuing a Digital Insurance Policy.

(7) Authorized (Legitimate) SSL certificate and other latest security certificates must be used and a purchase agreement must be submitted to Authority along with the yearly IT Audit report.

(8) The insurer has to establish standard transmission and encryption formats and non- repudiation safeguards for digital communications of data.

(9) Insurer shall employ responsibility and access limitation (access privileges) of the staff and authorized personnel as deemed necessary to protect confidential and private information and limit data breach.

(10) Any physical or digital access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back up sites and facilities and to the digital data communication network connecting the insurer, its approved persons and policyholders shall be controlled, monitored, and recorded.

(11) The insurer shall maintain regular file backup and have an efficient restoration strategy to ensure that its records are protected against loss or destruction. Also, arrangements shall be made for maintaining back up facilities at provincial locations as well.

(12) Firewall protection and other strong security measures must be ensured and configured in such a way that it refuses all access except those that are mandatory for the network and servers.

(13) All the server operating systems, databases, network devices, and other office automation software used by the insurer for Digital insurance policy infrastructure must have legitimate license keys.

(14) Standard password policies should be employed for server security, DIA, and software security i.e.

- (a) enforce a minimum character length of the password.
- (b) set password complexity guidelines.
- (c) enable session timeout for inactivity.
- (d) use a multi-factor authentication strategy.
- (e) set password expiration policy.



- (f) minimum login attempt strategy.
- (g) all login attempts should be monitored, and system logs should be recorded.

(15) There must be a provision of recording time stamp with other information of every account creation, E-Proposal submission, file upload, policy upload and other transactions and such information should be made available if requested by the Authority.

(16) Data and records amongst multiple systems should be reconciled.

(17) Cookies to record user's activity shall not be used in digital platform where Digital Insurance Policies are provided.

(18) Notifications of KYC approval, account login, policy approval, claim status or any events related to the process of issuing digital policy shall be provided to the DIA holder.

(19) Any personal data disclosure is prohibited on any medium or organization except asked by Authority.

(20) The insurer shall submit yearly reports regarding steps taken by it to maintain the privacy of data.

(21) The insurer shall have in place a detailed operations manual explaining all aspects of procedures and systems to issue digital policy, including the interface and method of transmission of information amongst the insurer, its authorized persons, and policyholders.

(22) The insurer shall implement security information management system like Security information and event management (SIEM)

(23) The server/computer should have a virus protection mechanism.

#### Chapter IV Miscellaneous

**15. Approval of Digital Policy:** Insurers who wish to issue insurance policies through digital medium apart from Annexure , shall file for approval at Authority along with the following documents:

- (a) cover letter,
- (b) board minutes,
- (c) procedure/process map to issue policy digitally,
- (d) Vulnerability Assessment and Penetration Testing (VAPT) report of system/platform/software used to issue digital policy,
- (e) digital policy issuance manual with digital claim settlement,
- (f) digital policy issuance system completion certificates by vendor/insurer whichever applicable.

**16. Preparation of Digital Platform of agent:** Insurers can prepare digital platform of agent for digital insurance policy. Such platform can have link with DIA and E-Proposal form with proper authentication with insured and without violating digital privacy of insured.

While doing so, the insurer is required to maintain profound IT security and make the agent responsible as per act and regulations.

17. **Inspection:** The Authority can inspect the system and arrangements for issuing policy through digital medium if deemed necessary.
18. **Rejection Right of Authority:** (1) The Authority shall reserve the right to reject the request pursuant to Guideline number 20 and may cancel the approval at any time if noncompliance of this guideline comes to notice of the Authority.  
(2) Insurers shall abide by the Insurance Act, Regulations and Directives, Guidelines, Circulars issued by Authority and relevant Acts of Government of Nepal in implementation of these guidelines.
19. **Discount in the Premium:** An insurer can offer a discount in the premium to the policyholders for policies issued through digital medium given that there is no involvement of agent in the purchase of such policy. Such a discount shall be as prescribed by the Authority.
20. **Right to Remove the Obstacle:** If any obstacle is encountered while carrying out the work as per these guidelines, the Authority shall have the right to remove the obstacle, interpret this guideline and issue clarification.

**Annexure**

**(Related to Guideline Number 5(5) of this Guideline)**

**Line of Insurance Business that can be issued Digitally.**

<b>Line of Business</b>		<b>Sum Assured</b>
Life Insurance	All term insurance	All Sum Assured and as per the company underwriting manual and limit
	Other than term insurance	Maximum Rs. 20,00,000, (subject to policies not requiring medical and financial underwriting limit)
Non-Life Insurance	Accident Insurance	All Policies
	Travel Medical Insurance	All Policies
	Motor Third Party and Comprehensive	All Policies
	Health Insurance	All Policies
	Property Insurance	All Policies
Micro Life and Micro Non-Life Insurance	All Portfolio and policies	As per regulatory Limit and as per company underwriting manual and limit

**Note:** Additional Products can be issued after approval from the Nepal Insurance Authority by clearly specifying their scope of authority and digital insurance product offerings.