

**DETAILED FINANCIAL PROFILE**

Balance Sheet

851 FISCHER HALLMAN RD KITCHENER Ontario N2M 5N8

Address of Branch

03591

2025-12-08

Transit

Date (YYYY MM DD)

FINANCIAL PROFILE OF: Karan Pravinbhai Gajjar

Name of client

AS OF:

2025-11-28

Date (YYYY MM DD)

ASSETS**SUMMARY**

Bank Accounts

Canadian Imperial Bank of Comm Institution	010 Bank ID	Transit	Account No.	Joint?	100.00 % Ownership %	\$9,721.63
Canadian Imperial Bank of Comm Institution	010 Bank ID	Transit	Account No.	Joint?	100.00 % Ownership %	\$62,845.17

Non-registered Investment

Institution	Bank ID	Transit	Account No.	Joint?	Ownership %
-------------	---------	---------	-------------	--------	-------------

Registered Investment

Canadian Imperial Bank of Commerce- Description						\$18,099.45
--	--	--	--	--	--	-------------

Vehicles

Description	Joint?	Ownership %
-------------	--------	-------------

Land/Buildings

Description	Municipal Assessment	Monthly Income	Joint?	Ownership %
-------------	----------------------	----------------	--------	-------------

Other

BUILDER DEPOSITS Description	Joint?	Ownership %	\$15,000.00
---------------------------------	--------	-------------	-------------

TOTAL ASSETS \$105,666.25**LIABILITIES TO RETAIN****SUMMARY**

Credit Cards

FLRENT Institution	\$2,152.00 Authorized credit	Joint? Monthly payment	\$0	\$0
-----------------------	---------------------------------	---------------------------	-----	-----

FLRENT Institution	\$2,152.00 Authorized credit	Joint? Monthly payment	\$0	\$0
-----------------------	---------------------------------	---------------------------	-----	-----

CIBC CARD SERVI

Institution	\$19,000.00 Authorized credit	Joint? Monthly payment	\$10.00	\$239.00
-------------	----------------------------------	---------------------------	---------	----------

Personal Loans

Institution	Bank ID	Transit	Account No.	Authorized credit	Joint?	Monthly payment
-------------	---------	---------	-------------	-------------------	--------	-----------------

Lines of Credit

Institution	Bank ID	Transit	Account No.	Joint?	Monthly payment
-------------	---------	---------	-------------	--------	-----------------

Mortgages

Institution	Bank ID	Transit	Account No.	Joint?	Monthly payment
-------------	---------	---------	-------------	--------	-----------------

Other

Description	Joint?	Monthly payment
-------------	--------	-----------------

LIABILITIES TO BE PAID FROM THE FINANCING

I authorize National Bank to:

- Pay off the debts mentioned below from my new financing
- Reduce the limit and close these debts if they are held at the Bank.

I understand that it is my responsibility to contact the financial institution to reduce my limit and close a debt mentioned below if it is held by a financial institution other than the Bank. I agree to do so as soon as possible after the opening of the new line of credit or the disbursement of the new loan.

I also understand that the amounts to be repaid to close a debt may be different from those shown below. For example, to account for daily interests until the date of repayment.

Credit Cards

Institution	Account #	Current Credit	Joint?	Monthly payment	Reimbursement Amount	New Credit	<input type="checkbox"/> Reduction of credit limit	<input type="checkbox"/> Credit Card to closed

Personal Loans

Institution	Account #	Current Credit	Joint?	Monthly payment	Reimbursement Amount	Balance	<input type="checkbox"/> Loan to closed

Lines of Credit

Institution	Account #	Current Credit	Joint?	Monthly payment	Reimbursement Amount	New Credit	<input type="checkbox"/> Reduction of credit limit	<input type="checkbox"/> Line of Credit to closed

Mortgages

Institution	Account #	Current Credit	Joint?	Monthly payment	Reimbursement Amount	Balance	<input type="checkbox"/> Loan to closed

Other

Description	Account #	Current Credit	Joint?	Monthly payment	Reimbursement Amount	Balance	<input type="checkbox"/> Reduction of credit limit	<input type="checkbox"/> To closed

TOTAL LIABILITIES **\$239.00**

EQUITY (Net Worth) **\$105,427.25**

MONTHLY INCOME

Salary (Main employment and other)	<u>\$8,583.33</u>
Other	<u> </u>
TOTAL	<u>\$8,583.33</u>

MONTHLY EXPENSES

Credit Card/Personal Loan/Mortgage	<u>\$10.00</u>
Other	<u> </u>
TOTAL	<u>\$10.00</u>

I certify that the information provided to the Bank is accurate.

I understand that the credit application related to this balance sheet will be analyzed by taking into account the upcoming changes to my assets or liabilities that I disclosed to you, if applicable.

2025-12-08

Date (YYYY MM DD)

0E0C14DDF725426
Signature of Applicant (ID: 2830811)

Karan Pravinbhai Gajjar

CLIENT PERSONAL INFORMATION

Karan Pravinbhai Gajjar Name of Client	20023828 Client No.	437-248-6266 Telephone No. (Home)		
204, Lisgar Ave, 307 Address	Tillsonburg City	Ontario Province	N4G 4L2 Postal Code	
2025-10-30 Since	Tenant Residential Status	English Communication Language	2025-10-30 Client since	
1996-08-11 Date of Birth (YYYY MM DD)	29 Age	Single Civil Status	0 Number of dependents	\$8,583.33 Monthly Income
204,Lisgar Ave,307 Previous Address	Tillsonburg City	Ontario Province	N4G 4L2 Postal Code	

Legal Action

EMPLOYMENT INFORMATION

FPT CANADA INC. Employer	Permanent Full-Time Employment Type	Software developer Occupation	2021-11-24 Date Started (YYYY MM DD)
800 Rue Du Square-Victoria Montréal H3C 0B4 QC CA Address of Employer		514-565-5000 Telephone No.	9999-12-31 Date Ended (YYYY MM DD)

Certificate Of Completion

Envelope Id: 746D6AF9-C6D5-4958-AC78-B91987E90CEB

Status: Completed

Subject: Please Sign Financial Profile Document

Source Envelope:

Document Pages: 3

Signatures: 1

Envelope Originator:

Certificate Pages: 3

Initials: 0

BANQUE NATIONALE / NATIONAL BANK

AutoNav: Enabled

800 Saint-Jacques Street

EnvelopeD Stamping: Enabled

Montreal, QC H3C 1A3

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

ECM.esig.prd@bnc.ca

IP Address: 142.225.32.218

Record Tracking

Status: Original

Holder: BANQUE NATIONALE / NATIONAL BANK

Location: DocuSign

12/8/2025 5:33:27 PM

ECM.esig.prd@bnc.ca

Signer Events

Karan Pravinbhai Gajjar

gajjar5113@gmail.com

Security Level: Email, Account Authentication
(None), Authentication

Signature

Signed by:

Karan Pravinbhai Gajjar
0E0C14DDF725426...

Timestamp

Sent: 12/8/2025 5:33:28 PM

Viewed: 12/8/2025 6:22:16 PM

Signed: 12/8/2025 6:22:33 PM

Signature Adoption: Pre-selected Style

Using IP Address:

2607:fea8:44e2:1f00:895c:79d3:2bd3:18dc

Authentication Details

SMS Auth:

Transaction: 28ffb125-5b62-491c-8c64-43a57337977a

Result: passed

Vendor ID: TeleSign

Type: SMSAuth

Performed: 12/8/2025 6:22:09 PM

Phone: +1 437-248-6266

Electronic Record and Signature Disclosure:

Accepted: 12/8/2025 6:22:16 PM

ID: 3a8a2600-5ee1-4edb-805c-71d3999c77d6

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	12/8/2025 5:33:28 PM
Certified Delivered	Security Checked	12/8/2025 6:22:16 PM
Signing Complete	Security Checked	12/8/2025 6:22:33 PM
Completed	Security Checked	12/8/2025 6:22:33 PM

Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

Any agreement signed using DocuSign will be deemed as duly and validly delivered and be deemed to be an original and valid document and will have the same legal effect as an agreement signed by hand. Electronic signatures will be deemed originals and compliant with applicable law.



800 Saint-Jacques Street, office 16701 Montreal (Quebec) H3C 1A3

**INSURANCE APPLICATION FOR CONSUMER
LOAN – MORTGAGE LOAN**Life, critical illness and accidental dismemberment, disability
Nº 70004B20 (2020-04-19)**REASON FOR INSURANCE APPLICATION**

- | | |
|--|--|
| <input type="checkbox"/> New loan application | <input type="checkbox"/> Refinancing of a National Bank loan - Indicate the number of the refinanced loan NA _____ |
| <input checked="" type="checkbox"/> Builder loan | <input type="checkbox"/> Adding new coverage (You already have life insurance) |

YOUR PERSONAL INFORMATION

Gajjar

Last name

1996-08-11

Sex

 M F

Date of birth (YYYY MM DD)

Karan Pravinbhai

First name

GAJJK039188001

Client No.

204 Lisgar Ave, 307, Tillsonburg, Ontario, N4G 4L2

Complete address, including postal code

gajjar5113@gmail.com

Email

LOAN INFORMATION

3000528490	\$559,999.97	2025-12-04
Reference No.	Authorized loan amount (or loan balance on insurance application date)	Approval date

CHOICE OF INSURED PERCENTAGE

Loans of \$300,000 or less – 100% insured only

Loans greater than \$300,000 - Choose one (If not checked, 100% of the loan amount will be insured)

- | | |
|---|--|
| <input type="checkbox"/> I choose to insure 100% of the total loan amount | <input type="checkbox"/> I choose to insure 50% of the total loan amount |
|---|--|

The percentage chosen applies to all coverage you signed up for.

The insured amount must not be higher than the maximum amount for each type of coverage. See section 3 of the certificate for more details.

CHOICE OF INSURED PAYMENT

The insured payment is the amount of the scheduled payment to repay your mortgage loan.

If you have selected an insured percentage, it also applies to the insured payment.

CHOICE OF THE INSURANCE START DATE

Choose one. If not checked, the approval date will be applied by default.

- | | |
|--|--|
| <input type="checkbox"/> Approval date | <input type="checkbox"/> Disbursement date (We will collect premiums no later than 6 months after the approval date) |
|--|--|

Your monthly premium: \$0.00 (including tax, if applicable)

ELIGIBILITY**You can apply for life insurance if:**

- You are between 18 and 64 years old and
- You are living in Canada or in the United States and
- You are a borrower, co-borrower, guarantor or endorser of the National Bank loan.

You can apply for critical illness and accidental dismemberment insurance if:

- You have signed up for life insurance.

You can apply for disability insurance if:

- You have signed up for life insurance
- You can answer "Yes" to the following 2 questions:

- In the past 4 weeks, have you completed at least 60 hours of remunerated work, or, if you are self-employed, have you generated a gross employment income of at least \$10,000 during the last fiscal year?
- Can you confirm that **you are not** on unemployment, a leave of absence or unemployed and that **you are not receiving** income replacement benefits (e.g., benefits as a result of a work-related accident or parental leave)?

If you answered "No," you CANNOT apply for disability insurance.

Yes	No
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

FPT CANADA INC.

Present employer's name

2021-11-24

Employed since (YYYY MM DD)

APPLICATION – WAIVER – INELIGIBILITY - MANDATORY SIGNATURE

	I request	I waive	I am not eligible for
Life insurance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Critical illness and accidental dismemberment insurance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Disability insurance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2025-12-08

Karan Pravinbhai Gajjar

Date (YYYY MM DD)

0E0C14DDF725426...
Your Signature ([ID: 1632621](#))**TOBACCO USE OVER THE PAST 12 MONTHS**

Please answer this question honestly and accurately. Otherwise, your insurance will be cancelled.

Yes	No
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

INSURABILITY - MANDATORY SIGNATURE ON THE NEXT PAGE**IMPORTANT****Answer honestly and accurately.**

Answering "Yes" to one of the questions does not mean coverage will be automatically declined.

Any false statement, whether intentional or not, could result in the denial of a claim or cancellation of your insurance.

If in doubt about the answer you need to provide, it is preferable to answer "Yes." One of our representatives will then contact you for a more detailed questionnaire in order to clarify the information.

Identify the category to which you belong using this table:

AMOUNT	AGE	PROCESS
From \$0 to \$150,000	Age 18 to 54	<p>Answer the questions in section A) SIMPLIFIED QUESTION.</p> <p>If at least one of the situations applies to you or in case of doubt:</p> <ul style="list-style-type: none"> > answer "Yes," and > complete the C) ADDITIONAL INFORMATION section. One of our representatives will contact you to complete a detailed questionnaire. <p>If you answered "No" to all the questions in the HEALTH DECLARATION, YOU ARE INSURED based on the accuracy of the information you provided.</p>

AMOUNT (continued)	AGE (continued)	PROCESS (continued)
From \$0 to \$500,000	Age 55 or older	Answer the questions in section B) HEALTH DECLARATION . In case of doubt: > tick "Yes," and > complete the C) ADDITIONAL INFORMATION section. One of our representatives will contact you to complete a detailed questionnaire.
From \$150,001 to \$500,000	Age 18 to 54	
From \$500,001 to \$1,000,000	Age 18 to 44	If you answer "No" to all the questions in the HEALTH DECLARATION, YOU ARE INSURED based on the accuracy of the information you have provided. You do not need to provide additional proof of insurability.
From \$500,001 to \$1,000,000	Age 45 or older	Go directly to section C) ADDITIONAL INFORMATION . One of our representatives will contact you to complete a detailed questionnaire.

A) SIMPLIFIED QUESTION	Yes	No
Have you ever:		
<ul style="list-style-type: none"> Had cancer, a heart attack or a stroke? Submitted a life, critical illness or disability insurance application that was: <ul style="list-style-type: none"> refused, deferred or cancelled; or issued with an exclusion or additional premium? OR 		
Over the past 5 years:		
<ul style="list-style-type: none"> Did you miss work due to disability for a period of more than 4 consecutive weeks? 	<input type="checkbox"/>	<input type="checkbox"/>
B) HEALTH DECLARATION		
a) In the past 3 years:		
<ul style="list-style-type: none"> Have you consulted, had a follow-up or been treated by a physician or another health care professional, or have you taken medication for or had symptoms related to or do you suffer from any of the following health problems? <ul style="list-style-type: none"> - Heart or circulatory disorders - Stroke - Chest pains or angina - Blood disorders including cholesterol - Blood pressure disorders - Muscular dystrophy - Multiple sclerosis - Acquired Immune Deficiency Syndrome (AIDS), Human Immunodeficiency Virus (HIV) or any other disease or disorder of the immune system - Tumour or cancer - Digestive problems - Liver disorders - Intestinal disorders - Kidney disorders - Urinary tract disorders - Lung or respiratory disorders (including sleep apnea) - Genital, prostate or breast disorders - Neurological disorders - Diabetes or glucose intolerance - Psychological or psychiatric disorders (including depression, anxiety, adjustment disorder, etc.) 		
and for any of the following problems, only if you are applying for disability insurance		
<ul style="list-style-type: none"> - Fibromyalgia or chronic fatigue syndrome - Muscle, joint or bone disorders (including sprains, tendonitis, bursitis, epicondylitis, osteoarthritis, etc.) - Carpal tunnel - Neck, back or spinal column problems 		
<ul style="list-style-type: none"> Have you used drugs (including marijuana)? Have you used narcotics exceeding the recommended dosage? Have you received treatment or joined a rehabilitation program because of your alcohol consumption? Have you been advised by a health care professional to reduce your consumption of alcohol? Do you have more than 4 glasses of alcohol per day (28/week)? 	<input type="checkbox"/>	<input type="checkbox"/>
b) In the past 3 years, have you been hospitalized due to an accident or illness for more than 48 consecutive hours?	<input type="checkbox"/>	<input type="checkbox"/>
c) In the past 3 years, have you applied for life, disability or critical illness insurance that was subject to additional premiums or refused or issued with a restriction?	<input type="checkbox"/>	<input type="checkbox"/>
d) If you are only applying for critical illness insurance, please also complete questions a), b) and c).	<input type="checkbox"/>	<input type="checkbox"/>
Has one or more members of your biological family (father, mother, brothers or sisters) suffered from diabetes, cancer, a stroke or heart disease before the age of 60?	<input type="checkbox"/>	<input type="checkbox"/>

I acknowledge that I have read and answered the Simplified question or the questions in the Health Declaration.

Date (YYYY MM DD)

Your Signature (*ID:1632831*)

C) ADDITIONAL INFORMATION (To be completed by all clients)

A representative of National Bank Life Insurance Company may contact you. Please indicate the best time and telephone number at which to reach you.

Please note: although the questions regarding insurability pertain to your most recent history (3 to 5 years), our representatives may have questions about a longer timeframe.

If a detailed questionnaire is required, you may choose the desired language. Please indicate your preference: English _____

Day 437-248-6266
Phone No. _____ Ext. _____

Evening 437-248-6266
Phone No. _____ Ext. _____

COLLECTION, USE AND DISCLOSURE OF YOUR PERSONAL INFORMATION

The insurer collects, uses and discloses your personal information to:

- Confirm your identity
- Provide the loan insurance requested
- Prevent fraud, manage risk and comply with laws
- Help the insurer improve and develop its products and services and better understand its clients
- Enable the insurer, National Bank of Canada or its subsidiaries, to present offers and other promotional material from business partners, unless you choose not to receive them
- Any other purpose set out in the Privacy Policy of National Bank and its subsidiaries available at <https://www.nbc.ca/privacy-policy.html>

The policy mentions, among others, which information the Insurer collects, to whom it is communicated, and how it is used and stored, what your options and rights are, and how to manage your consent.

In order to verify your insurability for loan insurance, the Insurer may also collect information from any doctor, hospital, clinic, paramedical firm, service provider, agent, insurance company, or any other organization that holds information on you or your health status, including MIB, LLC., an organization that maintains a database of applicant information that insurers may consult as part of their underwriting insurance or a claim (see Notice concerning MIB, LLC.).

In addition, the Insurer may also disclose any information about your health or other relevant information about you to MIB, LLC. or its reinsurers.

Your personal information will be kept by the Insurer and its subsidiaries for a reasonable period of time following the end of the business relationship to comply with their legal obligations.

If you have any questions, please contact the:

Access to Personal Information Officer
by writing to 800 St-Jacques, Suite 16701,
Montreal, Quebec H3C 1A3.

YOUR DECLARATION AND AUTHORIZATION - MANDATORY SIGNATURE ON THE NEXT PAGE

Information that you must read and understand

- I can cancel the insurance within 30 days of signing the application. If I do so, the Insurer will refund all the premiums paid, if any, and the insurance will be considered void.
- Insurance is optional and I can cancel it at any time.
- I am bound by all the provisions of the group insurance policy.
- I confirm it is my wish that this insurance application and the insurance certificate as well as all related documents be drawn up in English. *Je confirme ma volonté que cette proposition d'assurance et le certificat d'assurance ainsi que tous les documents s'y rattachant soient rédigés en anglais.*
- (Quebec only – as of June 1st, 2023) The French version of this insurance application and the insurance certificate is available here: assurances-bnc.ca/documentation.html, under the Mortgage Loan Insurance section. I confirm having received this version. (Québec seulement – à partir du 1er juin 2023) La version française de cette proposition d'assurance et du certificat d'assurance est disponible ici: assurances-bnc.ca/documentation.html, sous la section Assurance prêt hypothécaire. Je confirme avoir reçu cette version.

Authorization for your personal information

- I hereby authorize the Insurer to use any information it has pertaining to me.
- The information that I provided to the insurer as part of this application are correct and I hereby undertake to advise the Insurer immediately in writing of any change in my personal information so that it can keep my file up to date.
- I authorize the Insurer and National Bank of Canada to use my Social Insurance Number for administrative purposes. I may revoke my authorization at any time by contacting the Insurer.
- I have read the conditions set out in the "Collection, use and disclosure of your personal information" section in this application and I accept them.
- I have read the Insurer's Privacy Policy.
- I understand that signing up for loan insurance means that I accept the conditions of this Policy.
- I understand that I can limit the collection, use and disclosure of my personal information as set out in this Policy.
- If I have provided personal information about another person, I confirm that I am authorized to do so.

Authorization for your personal information (continued)

- I authorize the insurer and its reinsurers to collect information pertaining to me from any physician, hospital, clinic, paramedical firm, service provider, agent, insurance company, MIB, LLC. or any other organization or institution.
- I authorize the Insurer or its reinsurers to disclose any information pertaining to me to MIB LLC. (Medical Information Bureau).
- I authorize the Insurer to disclose my contact information and any changes to it that I may subsequently provide, as well as my personal and financial information to National Bank of Canada and its subsidiaries so that they may send me offers, information or invitations likely to be of interest to me.
- I authorize the Insurer to disclose my information to its service providers when insurance-related services are available.

Pre-authorized debit application (PAD Agreement)

Personal Business

Frequency and amount of debits

- I authorize the Insurer to debit the insurance premiums from the bank account used for the loan payments at the same frequency as the loan payment.
- Each debit corresponds to a fixed amount, except if you make changes to the loan conditions.

Waiver, changes and recourse

- **I waive any other confirmation before the first payment.**
- **I waive my right to receive notification should the amount of the debit change.**
- I will notify the Insurer at least 5 days before the next scheduled debit, of any changes to the bank account information or to the date of the debit.
- I may revoke my authorization at any time, subject to providing 30 days' notice. If I need additional information on the cancellation process, I may contact National Bank, the Insurer or go to www.payments.ca.
- I have certain recourse rights if a debit does not comply with this agreement. For example, I am entitled to reimbursement of any debit that is not authorized or is not consistent with this current agreement. If I need additional information on my recourse rights, I may contact National Bank, the Insurer or go to www.payments.ca.

YOUR COMMITMENT TO ACCURACY OF INFORMATION

- **I confirm that the answers and information provided in this application, including the sections on "Eligibility", "Tobacco use over the past 12 months" and "Insurability" are accurate and complete.**
- **I understand that any omission or misrepresentation may result in the cancellation of my insurance.**
- I have received and read all the information in this insurance application and the certificate of insurance.
- I confirm having received the fact sheet, summary and details on the coverage and the procedure to be followed to submit a claim.
- I understand that this insurance is optional. I choose the coverage(s) under this insurance that best suit(s) my situation and financial needs.

Date (YYYY MM DD)

Your Signature (*ID:1632851*)

DECLARATION OF WITNESS

I declare that I was present when this application was completed and witnessed all signatures thereon. For enrolment via phone or using an electronic signature: I have provided clear instructions on how to complete and sign this application.

I have submitted the fact sheet, certificate of insurance and the summary.

2025-12-08

Khalid Ahmad Ashraty

Date (YYYY MM DD)

Employee's first and last name

03591

Transit

TABLE OF CONTENTS

1.	Before we get started	3
1.1	Keep the following 6 rules in mind as you read this document:	3
1.2	Your insurance contract includes 2 documents:	3
1.3	Insurance is optional	3
1.4	You cannot designate a beneficiary	3
2.	Conditions to be insured	3
2.1	You must meet specific criteria (eligibility conditions)	3
2.2	We will ask you questions about your health and lifestyle (insurability)	4
2.2.1	Any false statement about your medical history could result in the cancellation of your insurance	4
2.2.2	Any false statement about your tobacco consumption will result in the cancellation of your insurance	4
2.2.3	You are covered against certain accidents while your file is under review	5
3.	Coverage offered and maximum amount we pay for each type of coverage	5
4.	Life insurance	5
4.1	Amount we pay in case of death	5
4.2	CAUTION- EXCLUSION in the event of suicide within 2 years of the signature of the insurance application	6
5.	Critical illness insurance	7
5.1	What we mean by cancer (life threatening)	7
5.1.1	CAUTION- EXCLUSIONS regarding cancer	7
5.2	What we mean by heart attack	8
5.2.1	CAUTION- Exclusions regarding heart attacks	8
5.3	What we mean by stroke	8
5.3.1	CAUTION- EXCLUSIONS regarding strokes	8
5.4	Amount we pay if one of the critical illnesses covered is diagnosed	8
6.	Accidental dismemberment insurance	10
6.1	What we mean by accidental dismemberment	10
6.2	Amount we pay in case of accidental dismemberment	10
	Percentages based on the loss	10
7.	Disability insurance	11
7.1	What we mean by disability	11
	Conditions to be entitled to disability benefits	11
7.2	CAUTION- EXCLUSIONS specific to disability	11
7.3	Amount we pay in case of disability	11
7.4	We maintain benefits if you refinance your loan during a disability	12
7.5	We pay benefits during a limited period	12
7.6	We cease paying disability insurance benefits in certain situations	12
7.7	We can resume payment of disability insurance benefits if you once again become disabled (recurrent disability)	13
7.8	We can terminate your disability coverage if you receive a permanent disability diagnosis	13
8.	CAUTION- General EXCLUSIONS	14
9.	Duration of insurance	14
9.1	Start	14
9.2	End	15
10.	Cost of insurance and payment of premiums	15
10.1	The cost of your insurance depends on several factors	15

10.2	Your insurance premiums are included in your mortgage payment*	15
10.3	Monthly premium rates for the mortgage loan	15
10.4	We reimburse the premiums collected in certain situations	16
11.	You must sign a new insurance application for a refinancing	16
11.1	During a refinancing, we may recognize your previous insurance if you are not insurable or not eligible	16
11.1.1	Recognized insurance amount	17
12.	You have the right to terminate your loan insurance at any time	17
12.1	You can call or write to us	17
12.2	We will reimburse the premiums paid if you cancel your insurance within 30 days of enrolment	17
12.3	We will not reimburse any premiums if you terminate your insurance more than 30 days after enrolment	17
13.	How do I make a claim and what happens then?	18
13.1	Timeframe to make a claim	18
13.2	We process and pay the benefits to National Bank within 30 days	18
13.3	We pay one set of benefits at a time	18
13.4	We adjust the premium rate in cases of incorrect declaration of age or sex	18
13.5	What you can do if you disagree with our decision about a claim	18
14.	Additional information	19
14.1	You or the Bank can obtain a copy of the documents that make up your insurance file	19
14.2	No dividends from surplus or profits	19
14.3	Designation of beneficiary	19
14.4	Limitation of actions— Specifics based on your province of residence	19
14.5	Notice concerning the MIB LLC. (Medical Information Bureau)	19
14.6	The confidentiality of your personal information is important to us- Access to personal information	20
15.	Complaint handling	20
16.	Autorité des marchés financiers contact information (province of Quebec only)	20

Who we are

National Bank Life Insurance Company, a subsidiary of National Bank of Canada. We are friendly and dedicated, and here to help.

What we do

We create insurance products for the different types of loans offered by National Bank and to meet your coverage needs.

Why we do it

For you! So that you can enjoy life with peace of mind, knowing we are here for you if an unfortunate event happens.

1. Before we get started

1.1 Keep the following 6 rules in mind as you read this document:

- > "We," "us" and "our" designate the insurer: National Bank Life Insurance Company.
- > "You" and "your" designate the insured, i.e., the person who applied for loan insurance, meets the eligibility and insurability criteria and received a copy of this certificate.
- > We only insure loans granted by National Bank of Canada. This is the institution we are referring to when we mention "the Bank" or "National Bank."
- > In this certificate, the word "loan" refers to your mortgage loan.
- > For ease of reading, the singular includes the plural, and the masculine includes the feminine, and vice versa.
- > Words that are defined in an information box have the same meaning in the entire certificate.

1.2 Your insurance contract includes 2 documents:

- > Your copy of the insurance application: the form you completed and signed to apply for insurance, regardless of the method used (handwritten signature, voice signature, e-signature).

With this document, you can confirm the information that you gave us and we used, as applicable, to review your application and render a decision (the Bank also has a copy); and

- > Your insurance certificate, which sets out the details of your coverage as well as your rights and obligations.

These two documents should be kept in a safe place to refer to them as needed!

Note: The Summary also provides valuable information about your loan insurance!

1.3 Insurance is optional

You are not required to enrol in loan insurance.

- > If you decide to do so, you can cancel the insurance at any time.
- > If you cancel within 30 days of signing the insurance application, we will reimburse you all the premiums paid and the insurance will be considered never having been in effect.

1.4 You cannot designate a beneficiary

Any benefits we provide are first paid to the Bank to be applied in full to the insured portion of your loan. The payment terms and conditions are explained to you in the "Amount we pay..." section of each type of coverage.

2. Conditions to be insured

2.1 You must meet specific criteria (eligibility conditions)

When signing the insurance application, you must:

For life insurance

- > Be between the ages of 18 and 64;
- > Be living in Canada or the United States; and
- > Be a borrower, co-borrower, guarantor or endorser of the loan targeted by the insurance application.

For critical illness and accidental dismemberment insurance

- > Have enrolled in life insurance.

For disability insurance

- > Have enrolled in life insurance; and
- > Be a salaried employee and have worked 60 or more remunerated hours over the past 4 weeks; or
- > If you are self-employed, have generated a gross employment income of \$10,000 or more the previous fiscal year.

You CANNOT apply for disability insurance if you:

- > Are unemployed;
- > Are on leave of absence;

- > **Don't have a job; or**
- > **Receive income replacement benefits (because of parental leave, work accident, etc.).**

However, you could apply to add this coverage once you have returned to work.

2.2 We will ask you questions about your health and lifestyle (insurability)

Depending on your age and the insurance amount requested, you may have completed the health declaration or answered the simplified question in the insurance application. If we need more information on your health and lifestyle, we could ask you to meet these requirements or undergo the following tests:

- > Detailed questionnaire completed by phone
- > Paramedical examination conducted by a nurse
- > Physical examination
- > Electrocardiogram
- > X-ray
- > Blood test
- > Urine test
- > Any other test, including screening for HIV (AIDS) or certain drugs or medication

The information collected through these various means enables us to determine whether we can accept your insurance application. **It is therefore important to answer honestly and to the best of your knowledge.**

2.2.1 Any false statement about your medical history could result in the cancellation of your insurance

When making a claim, certain conditions can lead us to check the information you provided at enrolment about your health, family and medical history as well as your lifestyle.

If the information collected as part of the claim is different from the information you provided at enrolment and on which we based ourselves to accept your insurance application, we could cancel your insurance retroactive to its effective date. Any claim would then be impossible.

IMPORTANT TO KNOW

- > We pay for any examination we require. If you decide to undergo a medical examination we have not requested, you will be responsible for the cost.
- > If we do not obtain the information required to review the application, we will terminate the analysis of your application.
- > Your application will be refused if the information about your health or lifestyle prevents us from insuring you. In that case, we would reimburse you any premiums you may have paid.
- > In any case (acceptance or refusal), we will notify you in writing of our decision within 30 days of receiving all your insurability information.

2.2.2 Any false statement about your tobacco consumption will result in the cancellation of your insurance

If you smoke, even occasionally, or use nicotine replacement products (including electronic cigarettes), you must notify us when you sign the insurance application.

Once the insurance is in effect (but not during a claim), if you realize that you have given incorrect information about your consumption of tobacco or nicotine replacement products,(including electronic cigarettes) you can rectify this by contacting one of our customer service representatives.

It should also be noted that making a false declaration about tobacco consumption when making a claim can have significant consequences. If you declare yourself to be a non-smoker when you sign the application and the information we obtain as part of the claim shows that you were a smoker at that time, we will refuse the claim and cancel your insurance retroactive to its effective date.

IMPORTANT TO KNOW

In order to be considered a non-smoker, you must not have used tobacco or nicotine replacement products of any kind (including electronic cigarettes) during the 12 months preceding the date the insurance application was signed.

2.2.3 You are covered against certain accidents while your file is under review

We offer you coverage in case of an accident while we are in the process of analyzing your application, until such time as we render a decision or close your file.

This accident coverage is provided at no additional charge and is based on the coverage you have chosen.

Benefits are only payable if the accident causing the death, disability or dismemberment occurs after the date on which the insurance application is signed.

See subsection 9.1.

However, if a non-accidental event occurs, we will finalize the review of the insurance application. If it is accepted, we will process the claim.

In this certificate:

By "accident," we mean an event that arises exclusively from causes external to the body. It occurs in a violent, unexpected and involuntary way, and causes bodily injury. A physician must establish that the accident is truly the source of the bodily injury, not an illness or other cause.

By "illness," we mean a deterioration in health requiring regular, ongoing and curative medical care actively provided by a physician or other practitioner belonging to a health profession order. Such care must be considered satisfactory by the insurer.

3. Coverage offered and maximum amount we pay for each type of coverage

The loan insurance provided by National Bank Life Insurance includes 3 types of coverage:

- > Life insurance
- > Critical illness and accidental dismemberment insurance
- > Disability insurance

You may have opted to enrol in all types of coverage or just one or two, as needed. Your selection is indicated on the insurance application you signed, a copy of which was given to you with this certificate.

Loan over \$300,000

You can choose to cover 100% or 50% of your mortgage loan. Your selection at enrolment is indicated on the insurance application.

The percentage chosen applies to all types of coverage.

Coverage	Maximum amount
Life insurance	\$1,000,000
Critical illness and accidental dismemberment insurance	\$150,000
Disability insurance	\$3,000/month

The maximum amount indicated corresponds to the maximum payable per coverage for all insureds on the loan.

IMPORTANT TO KNOW

The maximum insurance amount you can have with National Bank Life Insurance is \$5,000,000 for all insurance products.

If you are paying premiums for an amount higher than the maximum amount per type of coverage, we will reimburse you the difference in premiums.

The maximum amount set out in case of disability does not include the reimbursement of insurance premiums.

4. Life insurance

Life insurance covers both natural death and accidental death.

4.1 Amount we pay in case of death

In case of death, we pay the Bank the insured balance as of the date of death, plus any interest accrued since that date.

If premium payments are overdue on the date of death, these premiums are deducted from the amount we pay.

For life insurance, the insured balance is:

For loans over \$300,000 with 100% coverage and loans of \$300,000 or less

- > The outstanding loan balance on the date of death

For loans over \$300,000 with 50% coverage

- > The outstanding loan balance on the date of death multiplied by 50%

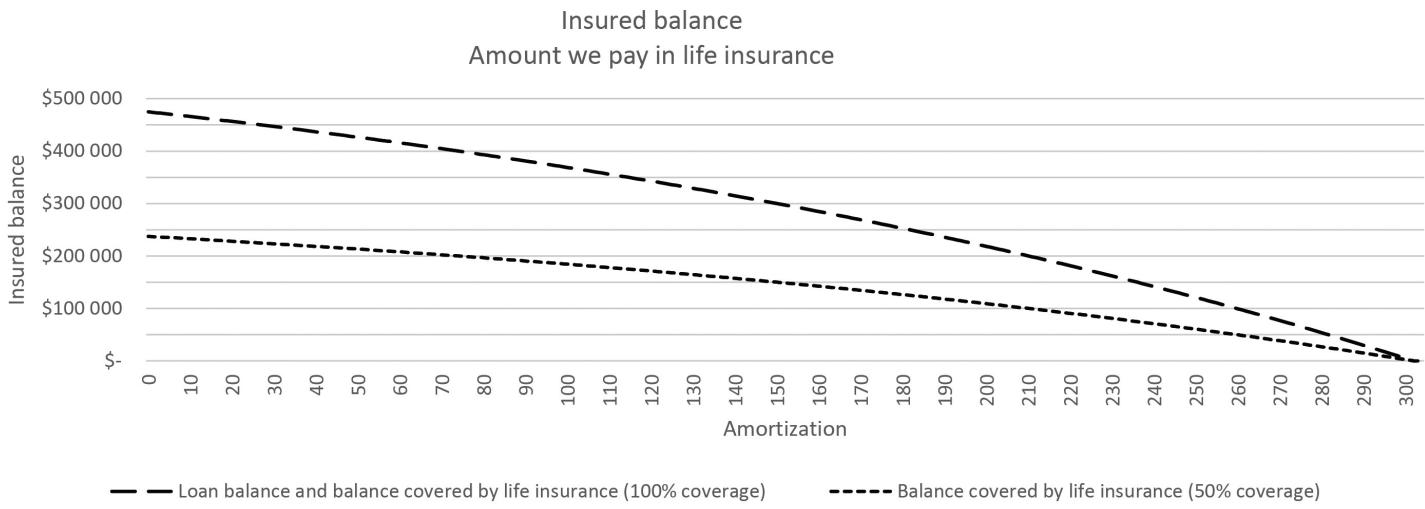
The insured balance:

- > cannot exceed \$1,000,000; and
- > does not include principal, interest, taxes or overdue premiums, under any circumstances.

Mark and Louise have had a mortgage loan for a few years. Fortunately, they decided to cover their debt with loan insurance so Mark is relieved not to have to bear the financial burden alone when Louise dies.

The amount we pay after accepting the claim is calculated as follows:

	100% coverage	50% coverage
Total loan amount at insurance enrolment	\$475,000	
Amount insured with life insurance	\$475,000	\$237,500 (\$475,000 X 50%)
Loan balance at the time of death	\$380,000	
Balance insured with life insurance on the date of death	\$380,000	\$190,000
Amount we pay	\$380,000	\$190,000



4.2 CAUTION - EXCLUSION in the event of suicide within 2 years of the signature of the insurance application

We will not pay any amount if your death is a result of suicide occurring within 2 years of the date your insurance took effect (see subsection 9.1).

Our liability will therefore be limited to reimbursing all the premiums paid. In that case, the insurance is cancelled retroactive to its effective date.

Consult section 8 to read about the other life insurance exclusions.

5. Critical illness insurance

We cover 3 types of critical illness:

- > Cancer (life threatening);
- > Heart attack; and
- > Stroke.

NOTE: The critical illness diagnosis must match the definition set out below.

5.1 What we mean by cancer (life threatening)

To be covered by this certificate, the cancer diagnosed must be a danger to your life and meet the following definition: definite diagnosis of a tumour, which must be characterized by the uncontrolled growth and spread of malignant cells and the invasion of tissue.

Types of cancer include carcinoma, melanoma, leukemia, lymphoma, and sarcoma.

This definition does not include the following:

- > Carcinoma in situ
- > Stage 1A malignant melanoma (melanoma less than or equal to 1.0 mm in thickness, not ulcerated and without Clark level IV or level V invasion)
- > Any non-melanoma skin cancer that has not metastasized
- > Stage A (T1a or T1b) prostate cancer

The diagnosis of cancer must be made by a specialist.

In this certificate, by "specialist," we mean a licenced medical practitioner who has been trained in the specific area of medicine relevant to the covered critical illness or accidental dismemberment condition for which the benefit is being claimed. They must be certified by a specialty examining board.

In the absence or unavailability of a specialist, and as approved by the insurer, a condition may be diagnosed by a qualified medical practitioner practicing in Canada or the United States.

The term specialist includes, but is not limited to: cardiologist, neurologist, oncologist, ophthalmologist, burn specialist and internist.

The specialist must not be the insured, the spouse or a relative of the insured or a business associate of the insured or of the insured's spouse.

5.1.1 CAUTION- EXCLUSIONS regarding cancer

We will not pay any benefits for cancer if, within 90 days of the insurance effective date, you have:

- > Presented signs, symptoms or been subject to investigations that lead to a diagnosis of cancer (covered or excluded by the insurance certificate), regardless of the date the diagnosis is made; or
- > Received a diagnosis of cancer (covered or excluded by the insurance certificate).

Furthermore, we will not pay any benefits in the following cases:

- > Lesions described as benign, pre-malignant, uncertain, borderline, non-invasive, carcinoma in-situ (Tis), or tumours classified as Ta
- > Malignant melanoma skin cancer that is less than or equal to 1.0 mm in thickness, unless it is ulcerated or is accompanied by lymph node or distant metastasis
- > Any non-melanoma skin cancer, without lymph node or distant metastasis
- > Prostate cancer classified as T1a or T1b, without lymph node or distant metastasis
- > Papillary thyroid cancer or follicular thyroid cancer, or both, that is less than or equal to 2.0 cm in greatest diameter and classified as T1, without lymph node or distant metastasis
- > Chronic lymphocytic leukemia classified less than Rai stage 1
- > Malignant gastrointestinal stromal tumours (GIST) and malignant carcinoid tumours, classified less than American Joint Committee on Cancer (AJCC) Stage 2

For the purposes of this certificate, the terms "Tis, Ta, T1a, T1b, T1 and AJCC Stage 2" are to be applied as defined in the American Joint Committee on Cancer (AJCC) Cancer Staging Manual (7th edition, 2010).

For the purposes of this certificate, the term "Rai staging" is to be applied as set out in KR Rai, A Sawitsky, EP Cronkite, AD Chanana, RN Levy and BS Pasternack: "Clinical staging of chronic lymphocytic leukemia," Blood 46:219, 1975.

Consult section 8 to read about the other critical illness insurance exclusions.

5.2 What we mean by heart attack

To be covered by this certificate, a heart attack must meet the following definition: definite diagnosis of a heart attack resulting from the death of a segment of the heart muscle due to obstruction of blood flow, that results in a rise and fall of biochemical cardiac markers to levels considered diagnostic of myocardial infarction, with at least one of the following:

- > Heart attack symptoms
- > New electrocardiogram (ECG) changes consistent with a heart attack
- > Development of new Q waves during or immediately following an intra-arterial cardiac procedure including, but not limited to, coronary angiography and coronary angioplasty

The diagnosis of heart attack must be made by a specialist (see the definition of "specialist" on p. 7).

5.2.1 CAUTION- Exclusions regarding heart attacks

We will not pay any benefits in the following cases:

- > Elevated biochemical cardiac markers as a result of an intra-arterial cardiac procedure including, but not limited to, coronary angiography and coronary angioplasty, in the absence of new Q waves
- > ECG changes suggesting a prior myocardial infarction, which do not meet the criteria for a heart attack as set out in this certificate

Consult section 8 to read about the other critical illness insurance exclusions.

5.3 What we mean by stroke (with persistent neurological deficits)

To be covered by this certificate, the stroke must meet the following definition: definite diagnosis of an acute cerebrovascular accident (CVA) caused by intra-cranial thrombosis or haemorrhage, or embolism, with:

- > Acute onset of new neurological symptoms; and
- > New objective neurological deficits on clinical examination.

persisting for more than 30 consecutive days following the date of diagnosis. These new symptoms and deficits must be corroborated by diagnostic imaging testing showing changes that, by their characteristics, location and timing, correspond to new neurological deficits.

The diagnosis of stroke must be made by a specialist (see the definition of "specialist" on p. 7).

For the purposes of the policy, neurological deficits must be detectable by a specialist and may include, but are not limited to, measurable hearing loss, measurable vision loss, measurable decline in neurocognitive function, objective loss of sensitivity, paralysis, localized weakness, dysarthria (pronunciation difficulties), dysphasia (language difficulties), dysphagia (difficulty swallowing), abnormal gait (difficulty walking), lack of balance, lack of coordination, or the appearance of seizures that are being treated.

Headache and fatigue will not be considered neurological deficits.

5.3.1 CAUTION- EXCLUSIONS regarding strokes

We will not pay any benefits in the following cases:

- > Transient ischaemic attacks
- > Intracerebral vascular events due to trauma
- > Ischaemic disorders of the vestibular system
- > Tissue death of the optic nerve or retina without total loss of sight in the eye involved; or
- > Lacunar infarcts which do not meet the definition of stroke as set out above

Consult section 8 to read about the other critical illness insurance exclusions.

5.4 Amount we pay if one of the critical illnesses covered is diagnosed

In the event of critical illness, we pay the Bank the insured balance as of the date on which the critical illness was diagnosed, plus any interest accrued since that date.

For critical illness insurance, the insured balance is:

For loans over \$300,000 with 100% coverage and loans of \$300,000 or less

- > The outstanding loan balance on the date on which one of the critical illnesses covered was diagnosed, up to a maximum of \$150,000.

IMPORTANT TO KNOW

For critical illness and accidental dismemberment coverage, the insured balance decreases starting when the balance insured with life insurance is less than \$150,000.

For loans over \$300,000 with 50% coverage, the lesser of the following amounts:

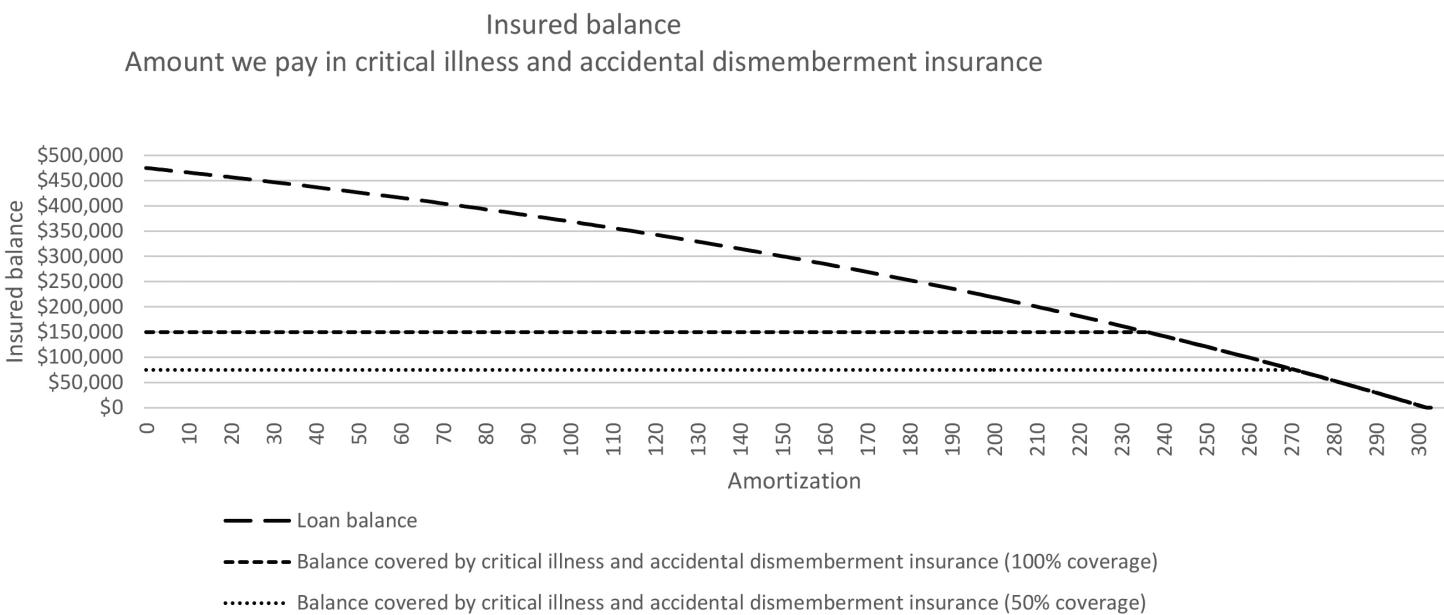
- The outstanding loan balance on the date on which one of the critical illnesses covered was diagnosed, multiplied by 50%; or
- \$75,000

IMPORTANT TO KNOW

In that case, the insured balance decreases starting when the balance insured with life insurance reaches the maximum stipulated for the coverage multiplied by 50% ($\$150,000 \times 50\% = \$75,000$). Subsequently, the insured balance decreases at the same pace as the loan balance.

In all cases, the insured balance:

- > cannot exceed \$150,000; and
- > does not include principal, interest or overdue premiums, under any circumstances.



The insured balance cannot be higher than the lesser of the following amounts:

- > The life insurance amount chosen at enrolment; or
- > The maximum amount set out for critical illness and accidental dismemberment insurance coverage (\$150,000).

On a beautiful fall morning, Michael collapses while he is raking leaves in his backyard: he has had a stroke. He is quickly taken to the hospital and receives appropriate care. Fortunately, Michael survives! His physician prescribes a few months of convalescence so that he can recover as much as possible before resuming his regular activities. Since Michael made the right decision to sign up for critical illness insurance when his advisor raised the issue with him, he contacts us after being discharged from the hospital to make a claim.

How we determine the amount to pay for this claim:

	100% coverage	50% coverage
Total loan amount at insurance enrolment		\$475,000
Loan balance at the time of the diagnosis		\$380,000
Balance with critical illness and accidental dismemberment coverage at the time of the diagnosis	\$150,000 (maximum amount)	\$75,000 (maximum amount)
Amount we pay	\$150,000	\$75,000

IMPORTANT TO KNOW

Payment of the critical illness benefits terminates the critical illness and accidental dismemberment insurance for all insureds.

However, if the amount paid for critical illness does not pay back the entire amount insured with life insurance, the life insurance remains in effect for all insureds on the amount insured with life insurance at enrolment less the amount paid for critical illness and accidental dismemberment insurance.

If Michael dies while his life insurance is still in effect, we will calculate the amount to pay as follows:

	100% coverage	50% coverage
Total loan amount at enrolment	\$475,000	
Amount insured with life insurance at enrolment	\$475,000	\$237,500
Loan balance on the date of the critical illness diagnosis	\$420,000	
Balance insured with life insurance on the date of the critical illness diagnosis	\$420,000	\$210,000
Balance insured with critical illness insurance (maximum amount)	\$150,000	\$75,000
Amount insured with life insurance (after the payment of critical illness insurance benefits)	\$270,000 (\$420,000 - \$150,000)	\$135,000 (\$210,000 - \$75,000)
Loan balance at the time of death	\$230,000	
Amount we pay in life insurance	\$230,000	\$115,000

If the payment of premiums is late on the date the critical illness is diagnosed, they are deducted from the amount we pay.

6. Accidental dismemberment insurance

6.1 What we mean by accidental dismemberment

Accidental dismemberment means to lose a limb or use of a limb, or to lose an eye or vision in one eye **further to an accident**. (See the definition of an accident on p. 5.)

By "loss of a limb", we mean:

- > Total amputation at or above the wrist or loss of use of a hand or an arm
- > Total amputation at or above the wrist or loss of use of a foot or leg
- > Total and irrecoverable loss of sight in one eye

By "loss of the use of a limb", we mean the total and irrecoverable loss of the limb in question, provided the loss continues for 12 consecutive months and is considered permanent.

The accident at the source of the dismemberment must occur while the insurance is in effect.

The loss or loss of use of a limb or an eye must be diagnosed by a specialist (see the definition of "specialist" on p. 7).

6.2 Amount we pay in case of accidental dismemberment

In case of accidental dismemberment, we pay the Bank an amount equal to the percentage of the insured loan balance calculated on the date of the accidental dismemberment diagnosis. The percentage is determined based on the loss suffered (see the table below).

The amount paid cannot exceed \$150,000.

For accidental dismemberment insurance, the insured balance is the outstanding balance of the mortgage loan calculated when a limb or use of a limb has been lost.

The insured balance decreases starting when the balance insured with life insurance is equal to \$150,000 (maximum amount set out for the coverage).

The insured balance:

- > cannot exceed \$150,000; and
- > does not include principal, interest, taxes or overdue premiums, under any circumstances.

Percentages based on the loss

Loss or loss of use	Percentage of insured balance
For each limb lost (including an eye)	25% (maximum 100%)
Both eyes	100%
Hemiplegia, quadriplegia or paraplegia	100%

Max loses an arm further to a work accident. Since Max has critical illness and accidental dismemberment insurance, he contacts us to make a claim. We will pay the following amount:

	100% coverage	50% coverage
Total loan amount at insurance enrolment	\$475,000	
Amount insured for critical illness and accidental dismemberment	\$150,000	\$75,000
Loan balance at the time the limb was lost	\$380,000	
Balance with critical illness and accidental dismemberment coverage at the time the limb was lost	\$150,000	\$75,000
Amount we pay (Insured balance X 25%)	\$37,500 (\$150,000 X 25%)	\$18,750 (\$75,000 X 25%)

IMPORTANT TO KNOW

In certain situations, we can pay the accidental dismemberment benefits AND the disability benefits for the same event (e.g., if the accidental dismemberment leads to the disability).

If the amount paid for the accidental dismemberment does not pay back the entire amount insured with life insurance, the life insurance remains in effect for all insureds on the amount insured with life insurance less the amount paid for accidental dismemberment. (see example in subsection 5.4).

The total amounts paid for dismemberments resulting from one or several accidents and for a critical illness cannot exceed the maximum amount payable of \$150,000.

7. Disability insurance

7.1 What we mean by disability

“Being disabled” or “being on disability” means that you are unable to perform the usual duties of your job for medical reasons. If you are unemployed, you are disabled if your physical or psychological health prevents you from doing normal activities for someone your age.

The disability must:

- > Be certified by a physician practicing in Canada or the United States;
- > Result from an illness or an accident suffered while the insurance is in effect (see the definitions of “illness” and “accident” on p. 4); and
- > Require ongoing medical care, deemed satisfactory by the insurer.

(See the definition of an accident and an illness on p. 5.)

Conditions to be entitled to disability benefits

- > Your disability must continue for at least 60 consecutive days. We will not pay any benefits during this time, which is the waiting period.

Note: An attempted return to work of a day or less during this period does not lead to a new waiting period.

- > During your disability, you cannot engage in any activity for which you receive financial compensation, regardless of how much it may be. Otherwise, we will refuse your claim and terminate benefits.

7.2 CAUTION- EXCLUSIONS specific to disability

In addition to the exclusions indicated in section 8, we do not pay any benefits for a disability that results directly or indirectly from the following conditions:

- > Alcoholism or drug addiction, unless these conditions are treated with a closed treatment program
- > Exclusions specific to the insured (if applicable), if we accept to insure you despite your medical history, medical condition, or travel to certain countries, by adding an exclusion with a rider.
- > Pregnancy: normal pregnancy
- > Back problems: back pain (dorsalgia), neck pain, or lower back pain (lumbago), which is only evidenced by the pain you feel and for which no objective diagnosis is possible, other than a diagnosis of normal arthrosis due to your age
- > Cosmetic care: Cosmetic treatment or surgery

Consult section 8 to read about the other disability insurance exclusions.

7.3 Amount we pay in case of disability

In case of disability, we pay the Bank an amount equivalent to the insured loan payment on the disability start date, including the insurance premium.

For disability insurance, "insured payment" means the amount of your loan payments, based on the insurance percentage selected at enrolment, if applicable. This amount includes the repayment of principal and interest.

Although insurance premiums are not part of the insured payment, we reimburse them to you in the event of a claim. However, they are not taken into account when calculating the maximum monthly amount payable for disability insurance.

For loans over \$300,000, the insured payment amount can be, based on the life insurance percentage chosen:

- > 100% of your mortgage payment, or
- > 50% of your mortgage payment.

	100% coverage	50% coverage
Mortgage payment amount	\$2,300/month	
Insured payment	\$2,300/month	\$1,150/month

The insured payment cannot be higher than the stipulated maximum of \$3,000 per month.

If a disability period is not as long as the period covered by a payment, we calculate the amount to be paid based on the number of days of disability.

Omar works in construction. He developed tendinitis in one of his shoulders and had to stop working for 3 months and 18 days. We calculated the amount to be paid for Omar's disability as follows, taking into account the 60-day waiting period.

	100% coverage	50% coverage
Loan payment	\$2,300/month	
Insured payment	\$2,300/month	\$1,150/month
Amount for the number of days of disability not part of a period covered by a payment (18 days)	$(\$2,300/30) \times 18 = \$1,380$	$(\$1,150/30) \times 18 = \690
Total for 1 month and 18 days	$\$2,300 + \$1,380 = \$3,680$	$\$1,150 + \$690 = \$1,840$
Amount we pay	\$3,680	\$1,840

7.4 We maintain benefits if you refinance your loan during a disability

In the case of a refinancing (i.e., when you increase your loan amount) while you are on disability, we will pay the payment that was insured before the refinancing, without exceeding the amount of the new payment. The benefits paid before the refinancing are calculated for the maximum benefit payment period related to the new insurance.

7.4.1 Renewal

If you renew the conditions of your loan (change in rate, amortization period, etc), we will pay the amount of your new payment up to a maximum of 120% of the amount of the payment before the renewal.

For example, your payment is \$500 before renewal and \$825 after.
 $(\$500 \times 120\%) = \600

The maximum payment that we will make for your disability further to the renewal will be \$600. You will have to assume the \$225 difference.

See subsection 7.5 for the maximum benefit payment period and section 11 for refinancing details.

7.5 We pay benefits during a limited period

For the full term of the loan and all insureds, we pay up to a maximum of 48 months of cumulative payments.

For a single disability, we pay up to a maximum of 24 months of consecutive payments.

IMPORTANT TO KNOW

Distinct disability periods must be separated by a return to work of **over 90 days**. Otherwise, it is considered the same disability period.

If you are unemployed, distinct disability periods must be separated by a return to normal activities for a person your age for over 90 days.

7.6 We cease paying disability insurance benefits in certain situations

Benefits cease when the earliest of the following events occurs:

Activities with financial compensation: When you engage in an activity for which you receive financial compensation, except if it is an attempted return to work of one day during the waiting period.

Maximum age: The last day of the month in which you turn 70.

Death: If you die or if we reimburse the insured loan balance due to the death of another insured.

End of disability: The date on which you are no longer disabled, based on the definition set out in this certificate.

Loan expiry: The date on which the loan is closed.

Critical illness or accidental dismemberment: We reimburse the amount insured with life insurance in full in case of a critical illness diagnosis or accidental dismemberment.

Maximum period: When we reimburse your insured loan payment for 24 months for a single disability, or 48 months for all insureds for the entire term of the loan.

Medical evidence not provided: If you fail to present the supporting documents we request within a reasonable timeframe (maximum of 1 year starting when the disability starts or our last communication, as applicable), and whether this is during the disability or at the beginning, or you refuse to undergo a medical examination or assessment by a rehabilitation consultant as we requested.

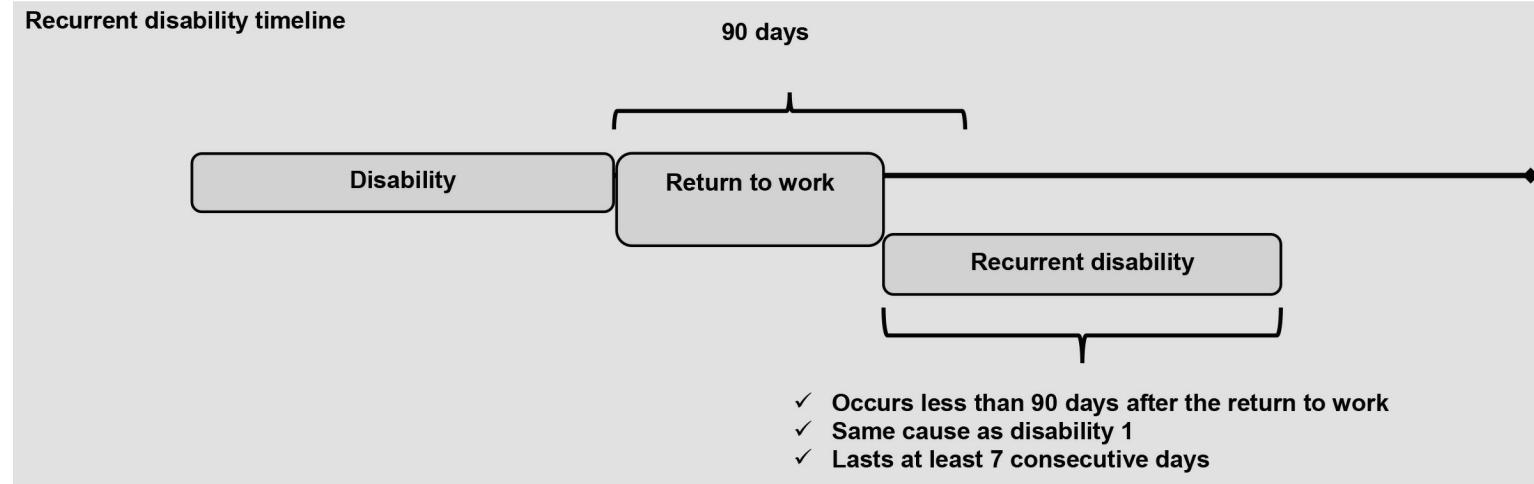
Return to work: The date on which you return to work part-time, full-time or gradually, or on temporary assignment, whether to carry out your normal duties for your job or any other job, including light work, unless it is an attempted return to work of one day during the waiting period.

7.7 We can resume payment of disability insurance benefits if you once again become disabled (recurrent disability)

The following 3 conditions must be met for us to resume repaying your insured loan payment:

1. The recurrent disability must occur within 90 days of your return to work or of normal activities for a person your age;
2. The relapse of this recurrent disability must be due to the same cause; and
3. You must be on leave of absence for at least 7 consecutive days.

Furthermore, you must provide us with medical evidence (e.g., a form completed by your attending physician). Claim requests for recurrent disability are subject to the same process as new claims.



If your recurrent disability meets all the criteria, we will start reimbursing your insured loan payment as we did before your return to work or to normal activities for a person your age.

Because it is the same disability, the duration of the recurrent disability is added to the previous disability to calculate the maximum period of 24 months.

You must present a new claim request if:

- Over 90 days have elapsed since your return to work or to normal activities for a person your age; or
- If your new disability occurs less than 90 days after your return to work and is attributable to another cause.

This new disability must continue for 60 days for us to pay benefits (waiting period).

7.8 We can terminate your disability coverage if you receive a permanent disability diagnosis

This avoids you having to pay premiums for coverage that no longer provides benefits. If this situation occurs, your life insurance and, if applicable, your critical illness and accidental dismemberment insurance, remain in effect.

8. CAUTION - General EXCLUSIONS

Specific exclusions for each type of coverage are set out in subsections 4.2, 5.1.1, 5.2.1, 5.3.1 and 7.2.

The following exclusions concern life insurance, critical illness and accidental dismemberment insurance as well as disability insurance.

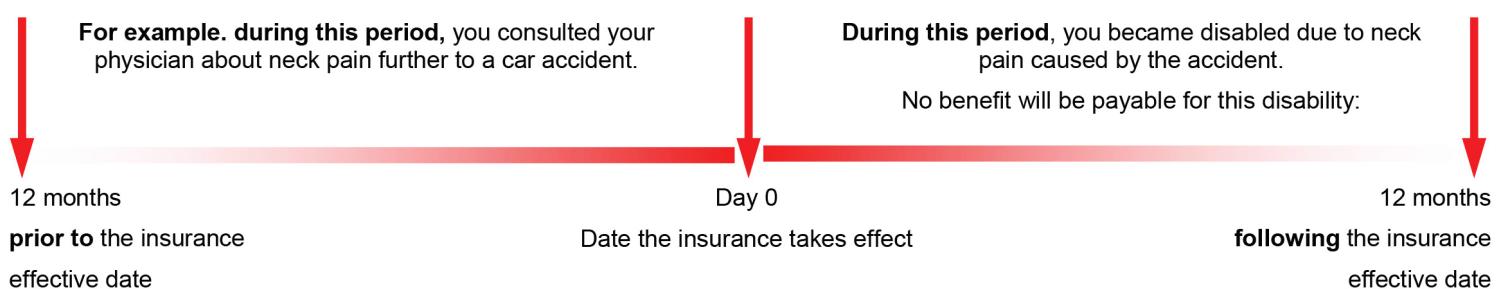
Pre-existing conditions

We do not pay any benefits if the death, critical illness, accidental dismemberment or disability occurs within 12 months of the insurance effective date, and that you have shown signs or experienced symptoms, contracted an illness, suffered an injury or from any other related cause, and that you have for this reason:

- Consulted or received treatment from a physician or other professional who is a member of a health care association or organization, or were referred for consultation or treatment purposes;
- Were subject to an examination or referred for an examination;
- Took medication or had medication prescribed to you; or
- Were hospitalized;

over the 12 months preceding the insurance effective date, whether there is a direct or indirect link between this pre-existing condition or illness and death, critical illness, accidental dismemberment or disability.

Example of pre-existing condition clause timeline



In addition, we do not pay any benefits when death, critical illness, accidental dismemberment or disability occurs under one of the following circumstances or if it is directly or indirectly related to one of the following circumstances:

- > **Criminal offence:** If you participate in a criminal offence or attempt to commit such an offence.
- > **Air travel:** If you actively participate in a flight in any type of craft which can climb and fly such as, but not limited to: an airplane, helicopter, glider or hot air balloon, whether as pilot, crew member, instructor or student.
- > **Riot:** If you actively participate in a civil uprising, riot or insurrection.
- > **War:** During a war or any act of war, whether or not you participated in it, unless you were acting as a member of the Canadian Forces or Canadian Forces Reserve.
- > **Drugs:** If you use narcotics or other medication, and exceed the dosage recommended by a physician or use drugs without a medical prescription.
- > **Attempted suicide or self-inflicted injury:** If you attempt suicide or injure yourself deliberately, regardless of your mental state at the time.
- > **Terrorism:** If you commit or attempt to commit an act of terrorism.

9. Duration of insurance

9.1 Start

The insurance will take effect on the later of the following dates:

- > The date the insurance proposal was signed; or
- > The date you have chosen and that is indicated on the application, i.e.,
 - The loan authorization date; or
 - The final disbursement date for the loan (if there is more than 6 months between the authorization and disbursement dates, we will start collecting premiums after 6 months)

9.2 End

In addition to the situations terminating the insurance which are described in this certificate, the insurance is terminated by one of the following events:

- > **Maximum age:** The last day of the month in which you turn 70.
- > **Cancellation:** The date on which you request cancellation of your insurance by phone, or the date on which the cancellation request is received at our offices.
- > **Assumption:** The date on which the loan (or part of the loan) is assumed by another obligor who is not insured by an insurance certificate for the loan.
- > **Death:** If we reimburse the insured loan balance further to a life insurance claim.
- > **Loan expiry:** The date the loan was closed.
- > **Critical illness or accidental dismemberment:** If we pay insurance benefits for a critical illness or accidental dismemberment and these benefits reimburse the entire amount insured with life insurance.
- > **Non-payment of premiums:** Loan payments are overdue by more than 3 months, or premiums if they are not included in the payment.

IMPORTANT TO KNOW

Critical illness and accidental dismemberment insurance as well as disability insurance are automatically terminated when life insurance ends.

10. Cost of insurance and payment of premiums

10.1 The cost of your insurance depends on several factors.

Your premium rate is determined based on:

- > Your age when the insurance application was signed
- > Your sex
- > Your consumption of tobacco or nicotine-replacement products (including electronic cigarettes)
- > Amount of your loan at enrolment

Different rates apply for each type of coverage. You will find a detailed rate table in subsection 10.3.

A 15% discount is applied on insurance premiums when there is more than one insured for life insurance, critical illness and accidental dismemberment coverage. This does not include tax on insurance. Tax rates can be viewed at [nbc.ca](#).

10.2 Your insurance premiums are included in your mortgage payment*

This means that if your loan payment is overdue so are your insurance premiums. After 3 months of overdue payments, the insurance is cancelled. *In certain situations, premiums may be collected in a separate transaction.

IMPORTANT TO KNOW

Your total insurance premiums are made up of premiums for each coverage in which you are enrolled.

Life insurance as well as critical illness and accidental dismemberment insurance remain fixed for the entire term of the loan.

Disability insurance premiums can change if you change your payment amount or the amortization of your loan.

10.3 Monthly premium rates for the mortgage loan

Note: We reserve the right to modify the premium pricing schedule at any time. The new schedule will then apply to all insureds.

The rates set out in this certificate are monthly rates. To obtain the premium that corresponds to the frequency of your payment, you need to multiply the monthly premium by one of these factors:

- > Weekly: 0.2301
- > Bi-weekly: 0.4603

Ages	Life (Rate per \$1,000)					Critical illness and accidental dismemberment (Rate per \$1,000)	Disability (Rate per \$10)
	\$0 - \$150,000 All	\$150,001 - \$1,000,000				\$0 - \$150,000 All	\$0 - \$3,000 per month All
		MNS	MS	FNS	FS		
18-25	0.12	0.12	0.19	0.09	0.14	0.17	0.18
26-30	0.12	0.12	0.20	0.09	0.16	0.20	0.18
31-35	0.14	0.14	0.22	0.12	0.19	0.27	0.25
36-40	0.21	0.20	0.27	0.18	0.24	0.34	0.30
41-45	0.30	0.28	0.41	0.25	0.34	0.46	0.40
46-50	0.44	0.41	0.64	0.36	0.49	0.72	0.48
51-55	0.59	0.54	0.93	0.46	0.67	1.12	0.61
56-60	0.79	0.71	1.30	0.59	0.88	1.56	0.78
61-64	1.07	0.96	1.72	0.82	1.19	1.90	0.98
65-69	1.07	0.96	1.72	0.82	1.19	1.90	0.98

10.3.1 Sample premium calculation

Jonathan is a 35-year old non-smoker.

He takes out a \$480,000 mortgage loan and chooses to sign up for life and disability insurance.

The monthly payment will be \$1,500. His house is located in Quebec, where the tax on insurance is 9%.

Here's how his insurance premiums will be calculated.

Life insurance

(Amount/1,000) X Premium rate X Tax
(\$480,000/ 1 000) X \$0.14 X 9% = **\$73.25**

Disability insurance

(Payment/10) X Premium rate X Tax
(\$1,500/10) X \$0.25 X 9% = **\$40.88**

Jonathan's total insurance premium will be \$114.13 per month.

10.4 We reimburse the premiums collected in certain situations

In addition to the specific situations set out in this certificate, we will reimburse any excess premiums collected.

You can request your premiums be reimbursed by phone or in writing. We will analyze your request and if we have indeed collected excess premiums, we will reimburse you for these premiums.

11. You must sign a new insurance application for a refinancing

Refinancing a loan means increasing the amount.

When you refinance your loan, you must sign a new insurance application to enable us to assess if we are still able to insure you for this new amount. The insurance for your current loan is then terminated, and the conditions of the new application apply:

- > Premiums are calculated based on your age and the new loan amount.
- > Restrictions and exclusions that involve a duration (e.g., suicide and pre-existing conditions) are reset to zero.

11.1 During a refinancing, we may recognize your previous insurance if you are not insurable or not eligible

If you are over 64 at the time of the refinancing, you are not eligible for insurance. If you are 64 or younger, you are eligible. However, a change in your health may prevent us from insuring you again.

Fortunately, there is a solution!

If the new application is refused because of your health, or if you are not eligible because of your age, we will insure you with the conditions of the new application (age, premium rate, exclusions, etc.) for the insured loan amount **before the refinancing**. We call this: recognition of previous insurance.

There are no steps to take. When we receive your new insurance application, we will review it and notify you in writing if we are able to recognize your previous insurance.

11.1.1 Recognized insurance amount

For life insurance and critical illness and accidental dismemberment insurance, the recognized insurance amount is calculated based on the insured balance of your loan before refinancing, compared to the amount of the loan after refinancing.

For disability insurance, the same ratio is applied to the new insured payment.

For loans over \$300,000, the insurance percentage chosen, indicated on the new insurance application, applies on the insured balance obtained with the recognition.

The recognized insurance amount cannot be higher than the maximum amount set out for each type of coverage.

Ronaldo and Anastasia are refinancing their loan to renovate their kitchen and bathroom.

When we receive Ronaldo's insurance application, we notice that his health status has changed since his previous application and we therefore cannot grant him insurance on his new loan.

However, we can recognize the insurance on the previous loan.

Loan details before and after the refinancing:

	Before the refinancing	After the refinancing
Authorized loan amount	\$175,500	\$250,000
Amount insured with life insurance	\$175,500	(\$175,500/\$250,000) = 70%

Ronaldo will therefore be insured for 70% of the amount of the new loan (or the loan payment, for disability insurance), calculated on the date of the event.

Recognition of previous insurance remains conditional on the accuracy of the information you provided when you submitted the first insurance application (on the previous loan). If certain details lead us to believe that the first insurance was granted with incorrect information, we could retroactively cancel the insurance and, if applicable, refuse a claim.

IMPORTANT TO KNOW

If you refinance a loan from another institution with the Bank, you must meet our eligibility and insurability criteria, and complete an insurance application. In case of refusal, we do not recognize the insurance held with another institution or another insurer.

12. You have the right to terminate your loan insurance at any time

12.1 You can call or write to us

To terminate your insurance:

- > Call our customer service at 1-877-871-7500; or
- > Write to us at:
National Bank Life Insurance
800 Saint-Jacques Street, office 16701
Montreal, Quebec H3C 1A3

12.2 We will reimburse the premiums paid if you cancel your insurance within 30 days of enrolment

If you cancel your insurance within 30 days of signing the insurance application, we will reimburse you the premiums collected, as applicable. The insurance will be cancelled and deemed never having been in effect.

12.3 We will not reimburse any premiums if you terminate your insurance more than 30 days after enrolment

Your insurance will be cancelled on the later of the following dates:

- > The date on which you indicate to us your intention to terminate the insurance
- > The date on which we receive your written request
- > The date on which you ask to have the insurance terminated, if you request it in advance.

We will not reimburse any premiums if you terminate your insurance, except for the reasons set out in this certificate.

13. How do I make a claim and what happens then?

13.1 Timeframe to make a claim

You must notify us quickly if you receive a diagnosis of critical illness or accidental dismemberment, or if you are in a disabled state for a period of more than 60 days. If you die, your estate will need to contact us.

We will send you forms to complete to make your claim. You must return them to us along with the required supporting documents, if applicable, within the following timeframes:

Timeframes to present claim documents and supporting documents

Critical illness, accidental dismemberment, disability	1 year from the diagnosis of critical illness, or accidental dismemberment, or the start of the disability. If you exceed this timeframe, you will no longer be entitled to receive benefits.
Life insurance	As soon as it is reasonably possible to do so.

To find out about the procedure, call our customer service at 1-877-871-7500. You can also consult our website at www.nbc-insurance.ca/claims.html.

13.2 We process and pay the benefits to National Bank within 30 days

We will process your request within 30 days of receiving the completed form and all required supporting documents.

If all the certificate conditions are met and we accept your claim, we will pay the benefits to the Bank within the same timeframe of 30 days.

13.3 We pay one set of benefits at a time

- > For life insurance and critical illness insurance, we pay the amount once for the entire term of the loan.
- > If 2 insureds are on disability at the same time, we will first pay the benefits for the disability leave expected to be the longest. If the first disability ends and the second insured is also entitled to benefits, we will continue the payment of the insured loan installments.
- > If an accidental dismemberment occurs simultaneously for more than one insured without it being possible to determine which of the insureds suffered the loss first, we will first pay the higher amount. If there is still an insured amount to reimburse on the loan, we will pay the following amounts, if applicable, until the amount insured with life insurance is refunded in full or the maximum insurable amount of \$150,000 has been reached.

13.4 We adjust the premium rate in cases of incorrect declaration of age or sex

If your age or sex has been incorrectly declared, we will adjust premiums based on the set rate for your age or sex when the insurance application was signed. If excess funds have been collected, we will reimburse you; if it is a shortfall, the amount will be deducted from the amount to be paid for your claim.

If your actual age exceeds the age at which your insurance ends, we will not pay any benefits and we will reimburse you all the excess premiums you paid after having turned the maximum age.

13.5 What you can do if you disagree with our decision about a claim

To contest a decision that we made as part of your claim request, you must contact us.

By phone:

Montreal: 514-394-9904

Toll-free: 1-866-817-4844

By email:

insurance@nbc.ca

You can also send us any document that could justify any review of our decision.

If we have not responded to your complaint, or if you are still not satisfied and want to continue with the process, you may at your discretion and at the same time:

- > Request a review of your file; or
- > Consult your legal advisor; or
- > Contact one of the following organizations:

Residents of the province of Quebec

Contact the Autorité des marchés financiers (AMF).

The contact information for the AMF is available in the

Autorité des marchés financiers - contact information below.

Residents of other provinces

Contact:

OmbudService for Life & Health Insurance (OLHI)

Toll-free: 1-888-295-8112

(Across Canada) or 416-777-9002 (in Toronto)

Website: olhi.ca

14. Additional information

14.1 You or the Bank can obtain a copy of the documents that make up your insurance file

Upon request, you or the Bank can obtain a copy of the policy, certificate, insurance proposal as well as any statement or document sent as evidence of insurability. Contact our customer service; one of our representatives will be happy to help you.

14.2 No dividends from surplus or profits

This insurance does not entitle you to receive any dividends from the surplus or profits we may declare.

14.3 Designation of beneficiary

This insurance certificate includes provisions revoking or restricting the right of the person covered by life insurance to designate beneficiaries to whom or for whose benefit insurance money is to be payable.

14.4 Limitation of actions - Specifics based on your province of residence

Residents of Alberta, British Columbia and Manitoba

Every action or proceeding against the insurer for the recovery of insurance money payable under the agreement is absolutely barred unless commenced within the timeframe set out in the Insurance Act.

Residents of Ontario

Every action or proceeding against an insurer for the recovery of insurance amounts payable under the agreement must be commenced within the timeframe set out in the Limitations Act, 2002 and its amendments.

Residents of New Brunswick

No action or procedure for recovery of a claim under the terms of this agreement can be brought against the insurer more than one year after the date on which the insured amounts became payable or would have become payable if the claim had been valid.

Residents of the province of Quebec

Every action or proceeding against the insurer for the recovery of insurance amounts payable under the terms of the agreement must be commenced within 3 years.

Residents of other provinces

For applicable limitation periods, consult your provincial regulatory body or your legal advisor.

14.5 Notice concerning the MIB LLC. (Medical Information Bureau)

Your insurability information will be treated in a confidential manner.

However, the insurer or its reinsurer may make a brief report thereon to MIB LLC. (Medical Information Bureau), a non-profit membership corporation of life insurance companies, which operates an information exchange on behalf of its members.

Upon request by a member insurance company to which you have applied for life or critical illness insurance coverage, or to which a claim is submitted, the MIB will supply such company with the information on its file. Upon receipt of a request from you, the MIB will arrange disclosure of any information it may have on file.

If the information in the MIB's files seems incorrect, you can ask for it to be corrected by writing to them at MIB LLC., 50 Braintree Hill Park, Suite 400, Braintree, MA 02184-8734, United States. Phone: 1-866-692-6901.

The insurer may also disclose information from its files to other life insurance companies to which you may apply for life or health insurance or to which a claim for benefits may have been submitted.

For more information on the MIB, consult the mib.com website.

14.6 Collection, use and disclosure of your personal information

The insurer collects, uses and discloses your personal information to:

- > Confirm your identity
- > Provide the loan insurance requested
- > Prevent fraud, manage risk and comply with laws
- > Help the insurer improve and develop its products and services and better understand its clients
- > Enable the insurer, National Bank of Canada or its subsidiaries, to present offers and other promotional material from business partners, unless you choose not to receive them
- > Any other purpose set out in the Privacy Policy of National Bank and its subsidiaries available at <https://www.nbc.ca/privacy-policy.html>. The policy mentions, among others, which information the Insurer collects, to whom it is communicated, and how it is used and stored, what your options and rights are, and how to manage your consent.

In order to verify your insurability for loan insurance, the Insurer may also collect information from any doctor, hospital, clinic, paramedical firm, service provider, agent, insurance company, or any other organization that holds information on you or your health status, including MIB, LLC., an organization that maintains a database of applicant information that insurers may consult as part of their underwriting insurance or a claim (see Notice concerning MIB, LLC.).

In addition, the Insurer may also disclose any information about your health or other relevant information about you to MIB, LLC. or its reinsurers.

Your personal information will be kept by the Insurer and its subsidiaries for a reasonable period of time following the end of the business relationship to comply with their legal obligations.

National Bank Life Insurance has implemented a series of measures to preserve the confidentiality of personal information.

We have put together an insurance file containing any personal information obtained in connection with your insurance application as well as information about any insurance claim under this insurance. Only employees or agents responsible for underwriting, administration, investigations and claims or the reinsurer, where applicable, have access to this file. All files are kept at our offices.

All persons authorized to do so (such as yourself or any person you authorize) may consult the personal information contained in the file and, if need be, request corrections by writing to:

National Bank Life Insurance Company, Access to Personal Information Officer, 800 Saint-Jacques Street, office 16701
Montreal, Quebec H3C 1A3.

For more information, consult our privacy policy nbc-insurance.ca/confidentiality.html.

15. Complaint handling

The client experience is our top priority.

No matter what you have to say, we're here to listen and provide assistance.

If the service you received didn't live up to your expectations, go to our website at www.nbc-insurance.ca/your-opinion.html to find out about our complaint handling process, or contact our customer service.

For more information, call us:

Montreal: 514-871-7500

Toll-free: 1-877-871-7500

16. Autorité des marchés financiers contact information (province of Quebec only)

For any additional information about the obligations of the insurer and distributor toward you, contact the Autorité des marchés financiers (AMF):

Autorité des marchés financiers

Place de la Cité, Cominar Tower

2640 Laurier, 4th Floor

Quebec City, Quebec G1V 5C1

Quebec City: 418-525-0337

Montreal: 514-395-0337

Elsewhere in the province of Quebec: 1-877-525-0337

Fax: 1-877-285-4378

autorite.qc.ca

No one may amend this certificate of insurance. All amended forms will be considered null and void. National Bank of Canada employees may at no time act as authorized agents of National Bank Life Insurance for the administration of these group insurance policies.

SUMMARY

Consumer loan insurance – Mortgage loan

10 important facts you should know about loan insurance

Do you have a mortgage loan with National Bank of Canada?

Have you considered what you would do if you were unable to make payments due to an unfortunate event?

Read this summary!

It presents key points about loan insurance.

Understanding these points will help you determine if this insurance product meets your needs so you can make an informed decision about your application.

This summary is an explanatory document: it is not part of the insurance contract. Only the completed application and the insurance certificate attached thereto will constitute the insurance contract.



For more details of the coverage, consult the insurance certificate, which is also available at nbc-insurance.ca › documentation.

- › Once you sign up, you are entitled to a 30-day review period. If you cancel your insurance before the end of that period, we will reimburse any premiums paid.



INFORMATION ABOUT THE INSURER

› National Bank Life Insurance Company

1100 Robert-Bourassa Blvd., 5th Floor
Montreal, Quebec H3B 2G7

Telephone Montreal area: 514-871-7500

Toll-free: 1-877-871-7500

Email: insurance@nbc.ca
nbc-insurance.ca

DISTRIBUTOR INFORMATION

› National Bank of Canada

600 De la Gauchetière St. West
Montreal, Quebec H3B 4L2

Telephone Montreal area: 514-394-5555

Toll-free: 1-888-483-5628

nbc.ca

Here are the 10 important facts you need know about loan insurance

1. There are 3 types of loan insurance coverage

1 In the event of your death, **life insurance** will help repay all or part of the balance of your mortgage loan, thereby freeing your family from one of the many obligations that come with the passing of a loved one.

2 **Critical illness insurance** also helps repay all or part of your loan if you are diagnosed with one of the following serious illnesses:

- › Cancer
- › Heart attack
- › Stroke

Moreover, **accidental dismemberment insurance** sees to the repayment of all or part of your loan if you lose a limb or permanently and irreversibly lose the use of a limb following an accident.

3 If you become unable to work or complete typical tasks for someone of your age due to an injury or illness, **disability insurance** can soften the blow of lost income by helping you make all or part of your mortgage payments. The disability must last at least 60 days before benefits can be paid out.

You can sign up for all three types of coverage or choose one or two. It's up to you!

However, you must sign up for life insurance to be eligible for critical illness or disability insurance.



You will find specific information for each protection in sections 4, 5, 6 and 7 of the insurance certificate.

2. Loan insurance covers the insured balance or insured payment of your loan, in whole or in part

For **life insurance or critical illness and accidental dismemberment insurance**, the insured balance is the balance of your mortgage loan as at the date of death or diagnosis of critical illness or accidental dismemberment, based on the insured percentage selected at enrolment and up to the maximum amount for that type of coverage (life: \$1,000,000; critical illness and accidental dismemberment: \$150,000).

For **disability insurance**, the insured payment is the payment of your mortgage payment, based on the insured percentage selected at enrolment and up to the maximum amount of \$3,000 per month.

› If the insured balance of your loan is **\$300,000 or less**, it will be 100% covered.

This means that in the event of death, diagnosis of a critical illness or accidental dismemberment, we will cover the insured balance of the loan at the time of the incident.

In the event of disability, we will cover the insured loan payment.

› If the insured balance of your loan is **greater than \$300,000**, you can opt to insure 50% or 100% of your loan.

This means that in the event of death, diagnosis of a critical illness or accidental dismemberment, we will cover the insured balance of the loan at the time of the incident according to the percentage selected.

In the event of disability, we will cover the insured loan payment according to the percentage selected.

The insurance percentage selected applies to all types of coverage you sign up for.

Maximum amount payable for each type of coverage

The amount payable for a claim cannot exceed the maximum for each type of coverage.

Life insurance	Critical illness and accidental dismemberment insurance	Disability insurance
\$1,000,000	\$150,000	\$3,000/month

If you are refinancing a loan and previous insurance coverage is recognized, we will apply the insurance percentage selected (100% or 50%) at refinancing on the insured balance of the previous loan without exceeding the maximum amount payable for each coverage.

For example:

	Insured amount/payment at refinancing	After refinancing
Loan amount	\$173,000	\$325,000
Loan payment	\$975	\$1,620

(cont.)	Insured at 100%	Insured at 50%
Insured balance for life insurance	\$173,000	(\$173,000 X 50%) \$86,500
Insured balance for critical illness and accidental dismemberment insurance	\$150,000	(\$150,000 X 50%) \$75,000
Insured payment for disability insurance	\$975	(\$975 X 50%) \$487.50

 See sections 3, 4.1, 5.4, 6.2, 7.3 and 11 of the insurance certificate for more details on the amount we pay for each protection.

3. Loan insurance involves exclusions

We may refuse to pay a claim because of the exclusions set out in the insurance certificate.

Please review them immediately. We've summed them up here for you:



WARNING – Exclusions

We will not pay any benefits in the following situations:

Life insurance

- › Suicide within 2 years of the insurance start date.

Critical illness insurance

Cancer

- › Some types of non-life-threatening cancer;
- › Signs, symptoms or examinations that led to diagnosis (regardless of the diagnosis date) or a cancer diagnosis received within 90 days of the insurance start date, whether the cancer is covered or excluded.

Heart attack

- › An increase in cardiac biochemical markers following a heart procedure;
- › The discovery of a past heart attack.

Stroke

- › Short-term altered brain function with no after-effects;
- › A stroke caused by trauma;
- › A lacunar infarct that doesn't meet the definition indicated in the insurance certificate.

Disability insurance

- › Alcoholism or addiction;
- › Pregnancy;
- › Back pain (if its existence is determined solely on pain you feel without an established cause);
- › Cosmetic care.

Concerning all protections

- › Pre-existing condition: Have you consulted a physician, or been treated or hospitalized for a medical condition within the 12 months preceding the start date of your insurance? Note that the exclusion for a pre-existing condition will apply if death, a disability or a critical illness diagnosis in relation to the condition occurs within the 12 months following the start date of your insurance;
- › Exclusion specific to the insured: Further to an analysis of your insurance application and the answers you have provided, we may offer to insure you while excluding:
 - Certain medical conditions,
 - Events that could arise during travel abroad,
 - Any other condition deemed too high-risk;
- › Participation in a criminal act or an attempt to commit one;
- › Active participation in the flight of any device capable of lifting off and travelling in the air—including but not limited to airplanes, helicopters, hang gliders and hot-air balloons—, be it as a pilot, crew member, instructor or student;
- › Active participation in a riot;
- › War;
- › Use of narcotics without a prescription or of medication beyond the prescribed dosage;
- › Attempted suicide or voluntary self-harm;
- › An act of terrorism you commit or attempt to commit.

Graphic example of a pre-existing conditions clause



During this period, you consulted your physician for neck pain. He prescribed you anti-inflammatories.



During this period, you became disabled and stopped working because of your neck pain. No benefits will be payable for this disability.



12 months before
the insurance start date

Day 0
Effective date of insurance

12 months after
the insurance start date



The specific and more detailed exclusions concerning each protection as well as the general exclusions are described in sections 4.2, 5.1.1, 5.2.1, 5.3.1, 7.2 and 8 of the insurance certificate.

4. You must meet certain criteria to be insured

To be eligible, you must, at the time of enrolment:

For life insurance:

- › Be 18 to 64 years old, inclusively;
- › Be living in Canada or the United States;
- › Be a borrower, co-borrower, guarantor or endorser of the insured loan.

For critical illness and accidental dismemberment insurance:

- › Have signed up for life insurance.

For disability insurance:

- › Have signed up for life insurance; and
- › Be employed and have worked 60 hours or more within the last 4 weeks for compensation; or
- › If you are self-employed, you must have generated a gross income of at least \$10,000 during the past fiscal year.

You may NOT apply for disability insurance on your loan if you:

- › Are on unemployment;
- › Are on a work stoppage;
- › Are jobless;
- › Receive income replacement payments (due to a disability, parental leave, work-related accident, etc.).

However, you can apply to add this type of coverage when you meet the eligibility criteria for indicated above.

Depending on your age and the amount of coverage requested, we will ask you some questions about your state of health and lifestyle.



See section 2 of the insurance certificate for more information.

5. The insurance premium payable is fixed for the duration of the loan

The premium is the amount you pay in order to be insured. As long as the terms and conditions of your loan do not change, your life, critical illness and accidental dismemberment insurance premiums will remain the same.

However, your disability insurance premium may change if your mortgage payment amount is adjusted.

We reserve the right to amend our premium rate scales at any time. If we do so, the premiums charged to all our insureds will change.

Your premium rate is based on a number of factors, including:

- › The insured amount;
- › Your age when you sign the insurance application;
- › Your sex;
- › Your use of tobacco products.

The insurance taxes of your Canadian province of residence will also apply.

With some exceptions, your insurance premium is included in your mortgage payment. It is therefore collected as part of the same transaction.

SAMPLE PREMIUM CALCULATION

William, 38-year-old man, non-smoker

\$375,000 mortgage

Monthly payments of **\$1,800**

Insured at 100%, life and disability insurance

Age	Life				Disability
	(Rate per \$1,000)				(Rate per \$10)
	\$0 to \$150,000	\$150,001 to \$1,000,000			\$0 to \$3,000 per month
Age	All	NSM	SM	SMF	SF
18-25	0.12	0.12	0.19	0.09	0.14
26-30	0.12	0.12	0.20	0.09	0.16
31-35	0.14	0.14	0.22	0.12	0.19
36-40	0.21	0.20	0.27	0.18	0.24
					0.30

Life insurance premium calculation

(Insured amount/\$1,000) X premium rate X taxes on insurance by province (Quebec: 9%)

$$(\$375,000/\$1,000) \times \$0.20 \times 9\% = \$81.75$$

Calculating the premium – Disability insurance

(Insured amount/\$10) X premium rate X taxes on insurance by province (Quebec: 9%)

$$(\$1,800/\$10) \times \$0.30 \times 9\% = \$58.86$$

Approximate total monthly premium: $\$81.75 + \$58.86 = \$140.61$



Consult the insurance certificate for premium rates and nbc.ca for tax rates.

6. Duration of insurance

Start

The insurance starts on the later of the following dates:

- a The date the insurance application is signed; or
- b Depending on the choice indicated on the application:
 - › The loan approval date; or
 - › The final loan disbursement date (may not be more than 6 months after approval); or
 - › For a new construction with single disbursement, the final loan disbursement.

If you are required to provide proof of insurability, we will notify you in writing of our decision within 30 days of receiving the documents needed to analyze your insurance application.

End

Insurance generally remains in effect for the entire loan duration, unless you decide to terminate your coverage.

Other circumstances also lead to the termination of the insurance, like refinancing, non-payment of premiums or when you reach the age of 70.



See section 9 of the insurance certificate for more information.

7. You'll have access to temporary accident coverage while we are studying your application

While we are analyzing your insurance application, you'll be covered in the event of accidental death, dismemberment or disability (depending on the coverage selected).

 See section 2.2.3 of the certificate for the definition of an accident and details of temporary coverage in the event of an accident.

8. We can refuse a claim and cancel your insurance if you make a false declaration

You must always provide accurate information on your health status, lifestyle and tobacco use, and any other information we deem necessary.

If, during a claim or at any other time during the insurance period, we receive information that differs from the information you initially provided, **we could refuse your claim and retroactively cancel your insurance** from its start date.

 See sections 2.2, 2.2.1 and 2.2.2 of the insurance certificate for more information.

9. How to file a claim and applicable timeframes

Loan insurance can give you peace of mind should the unexpected occur. Here's how to file an insurance claim.

1 Contact a member of our claims team:

Montreal: 514-394-9904
Toll-free: 1-866-817-4844

We'll open a file for you and send you the forms to be completed; or

Print the forms you need from the National Bank website at nbc.ca/insurance-claim.

2 Complete and sign the forms and send them, along with any documents needed to review your claim if applicable, to our offices at:

National Bank Life Insurance
1100 Robert-Bourassa Blvd., 5th Floor
Montreal, Quebec H3B 2G7
Email: insurance@nbc.ca

Timeframes for submitting claim forms and supporting documents

- › **Life insurance:** As soon as reasonably possible.
- › **Critical illness, accidental dismemberment or disability insurance:** Within one year following the critical illness or accidental dismemberment diagnosis or the beginning of the disability.

3 We will inform you of our decision after assessing your request and, if applicable, proceed with payment.

The typical waiting period to process a claim is approximately 30 days after all documents required for assessing the request have been received.

Do you disagree with a decision made regarding your claim?

Contact us:

By phone
Montreal: 514-394-9904
Toll-free: 1-866-817-4844

By email
insurance@nbc.ca

You can also forward us any document that could justify a revision of our decision. If we haven't addressed your complaint or if you're still dissatisfied and wish to pursue the matter further, you can take any of the following actions:

- › Request a revision of your file; or
- › Consult your legal advisor; or
- › Contact the following organization:

OmbudService for Life and Health Insurance (OLHI)

Phone, toll-free
Canada: 1-888-295-8112
Toronto: 416-777-9002

Online
olhi.ca

10. Loan insurance is optional and you are entitled to terminate it at any time

You can terminate your insurance at any time at no cost by calling us at 1-877-871-7500.

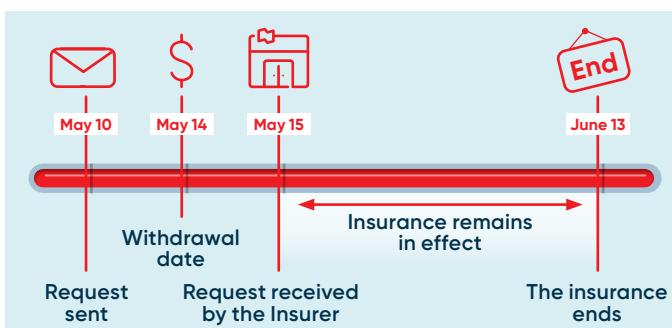
You can also send a written request to:

National Bank Life Insurance Company
1100 Robert-Bourassa Blvd., 5th Floor
Montreal, Quebec H3B 2G7
By email: insurance@nbc.ca

The insurance will end on the next premium payment date after the later of the following dates:

- › The date on which you choose to terminate your insurance coverage; or
- › The date on which we receive your termination request.

For example, in the image below, the insurance would remain in effect until June 13, since the insurer received the request to terminate the insurance after the current month's premium payment date.



If you terminate your insurance contract after the first 30 days, no premiums will be reimbursed and no grace period is granted.



The client experience is our top priority

We're here to listen and help, no matter what you have to say.

You can contact our Customer Service department at 1-877-871-7500 or visit at nbc-insurance.ca/your-opinion
to learn about our complaint management process, make a complaint and consult our policy on processing complaints.

Insurer: National Bank Life Insurance Company.
The NATIONAL BANK INSURANCE word mark and logo are trademarks of National Bank of Canada, used under licence by some of its subsidiaries.
© 2022 National Bank of Canada. All rights reserved. Any reproduction, in whole or in part, is strictly prohibited without the prior written consent
of National Bank of Canada.



Certificate Of Completion

Envelope Id: 335F1562-4847-4722-975B-BED63F306158

Status: Completed

Subject: Please Sign Creditor Insurance Document

Source Envelope:

Document Pages: 31

Signatures: 1

Envelope Originator:

Certificate Pages: 3

Initials: 0

BANQUE NATIONALE / NATIONAL BANK

AutoNav: Enabled

800 Saint-Jacques Street

EnvelopeD Stamping: Enabled

Montreal, QC H3C 1A3

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

ECM.esig.prd@bnc.ca

IP Address: 142.225.32.149

Record Tracking

Status: Original

Holder: BANQUE NATIONALE / NATIONAL BANK

Location: DocuSign

12/8/2025 5:32:51 PM

ECM.esig.prd@bnc.ca

Signer Events

Karan Pravinbhai Gajjar
gajjar5113@gmail.com

Signature

Signed by:

Karan Pravinbhai Gajjar
0E0C14DDF725426...

Timestamp

Sent: 12/8/2025 5:32:53 PM
Viewed: 12/8/2025 6:20:57 PM
Signed: 12/8/2025 6:21:38 PM

Security Level: Email, Account Authentication
(None), Authentication

Signature Adoption: Pre-selected Style
Using IP Address:
2607:fea8:44e2:1f00:895c:79d3:2bd3:18dc

Authentication Details

SMS Auth:

Transaction: 2c6b4708-881d-455e-b646-7c7f09bd87c9
Result: passed
Vendor ID: TeleSign
Type: SMSAuth
Performed: 12/8/2025 6:20:48 PM
Phone: +1 437-248-6266

Electronic Record and Signature Disclosure:

Accepted: 12/8/2025 6:20:57 PM
ID: 070a8e27-b230-405e-92c5-187faa85b84d

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	12/8/2025 5:32:53 PM
Certified Delivered	Security Checked	12/8/2025 6:20:57 PM
Signing Complete	Security Checked	12/8/2025 6:21:38 PM
Completed	Security Checked	12/8/2025 6:21:38 PM

Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

Any agreement signed using DocuSign will be deemed as duly and validly delivered and be deemed to be an original and valid document and will have the same legal effect as an agreement signed by hand. Electronic signatures will be deemed originals and compliant with applicable law.



Regulation

INFORMATION SECURITY

Document Code	35/2025/QDh/FSOFT - EN
Version	5.0
Effective Date	30-May-2025

Karan.Gajjar 2025-12-16 05:23:06

Code: Effective date: 30/05/2025 Version: 5.0	INFORMATION SECURITY REGULATION
--	--

TABLE OF CONTENTS

CHAPTER I. GENERAL REGULATION	3
Article 1. Applicable scope and Objects	3
Article 2. Definition and explanation of the terms.....	3
Article 3. Duties and responsibilities of functional departments, managers and staffs ...	4
CHAPTER II. INFORMATION SECURITY REGULATION	6
Article 4. Usage of confidential information.....	6
Article 5. Bringing information storage/processing asset, confidential information out of working areas.....	6
Article 6. Teleworking and mobile devices	6
Article 7. Non-disclosure commitments and trainings	7
Article 8. Personal owned device usage for work purposes.....	7
Article 9. Account and password management	7
Article 10. Entrance and exit at working areas	8
Article 11. Usage of cameras and recording devices	8
Article 12. Usage of printers, paper shredders	8
Article 13. Usage of fax machines	9
Article 14. Preservation of hard copy documents and records	9
Article 15. Information and document transfer.....	9
Article 16. Usage of computers and other technology devices	9
Article 17. Usage of software/extension.....	9
Article 18. Usage of mobile devices, network devices and peripherals.....	10
Article 19. Usage of Company emails	10
Article 20. Usage of Intranet, information systems, servers and Internet.....	11
Article 21. Antivirus and system update.....	11
Article 22. Usage of customer's assets.....	12
Article 23. Use of social media	12
Article 24. Information security incident management.....	12
CHAPTER III. HANDLING OF INFORMATION SECURITY VIOLATION	13
Article 25. Basis of the handling information security violation	13
Article 26. Forms of handling information security violation	13
Article 27. Handling of information security violation	13
CHAPTER IV. IMPLEMENTATION PROVISIONS.....	13
Article 28. Implementation responsibility	13
Article 29. Amendment and suplementation	13
APPENDIX OF BONUS DEDUCTIONS.....	14

CHAPTER I. GENERAL REGULATION

Article 1. Applicable scope and Objects

This regulation is applied to FPT Software Limited Company (hereafter called Company) and Subsidiary Companies.

Applicable objects are all staff of Company (hereafter called Staff), who signed Probationary Contracts, Short-term training contracts, On-the-Job training contracts, Seasonal labor contracts, Contracts for certain jobs for less than 12 months, Limited contracts for from 12 months to 36 months, or Unlimited contracts with Company.

Article 2. Definition and explanation of the terms

2.1. **Confidential information** means all non-public information, data, news, events, facts, ideas, judgment, knowledge of assets, or whatsoever in any form similar, related to production and business activities of the Company; or of customers/partners that are exchanged during business transaction process with the Company. Applicable scope includes but not limited as following:

- 2.1. 1. Software products of Company and customers/partners, including:
 - a) Initial surveys and analysis design documents,
 - b) Design documents, product modules,
 - c) Database, computer programs, including source codes, object codes,
 - d) Software development tools such as database, programming languages, translation programs, supplementary programs,
 - e) Software packages, usage guild lines,
 - f) Interface origin of software products, including the Company's websites and Company's websites designed for customers/partners.
 - 2.1. 2. Designs/solutions and installation/deployment procedures for any information technology product lines or for any customers/partners and relevant documents
 - 2.1. 3. Information system integration solutions and technological solutions deployed for Company, customers/partners.
 - 2.1. 4. Reports or summary documents of solution/design researched or developed by Company
 - 2.1. 5. Confidential information related to the market, customers, finance and others, which is specifically analyzed, developed or deployed by Company.
 - 2.1. 6. Personally Identifiable Information (PII) of customers or of customer' clients and other personal information, if any, commissioned by the customers for work purposes.
 - 2.1. 7. Personally Identifiable Information (PII) of staff, including but not limited to, name, date of birth, birthplace, personal identification number, social security number, account, email address, Internet Protocol address, web cookie, home address, telephone numbers, salary, job position, education, training history, curriculum vitae, children, parents, etc.
 - 2.1. 8. Production procedures, including all constitutive documents such as process descriptions, product descriptions and templates.
 - 2.1. 9. Written information or electric information which is marked "Confidential" or "Internal Use" or other similar forms.
- 2.2. **Company's partners:** are individuals, communities or organizations, which run the same or similar products/services to Company, which have the same customer targets or partner targets as the Company and share the benefits with Company.
 - 2.3. **Company's competitors:** are individuals, communities or organizations, which run the same or similar products/services to Company, which have the same customer targets or partner targets as the Company but do not share the benefits with Company.
 - 2.4. **Company's customers:** are individuals, communities or organizations, which purchase Company's products/services.
 - 2.5. **Third parties:** are individuals, communities or organizations, except Company itself and the staff who possess the confidential information.

- 2.6. **Mobile devices:** Handheld or notebook-sized devices that allow people to store or send information or connect to the Internet from wherever they are, include but do not limit laptop, tablets, mobile phones, external memory devices such as USB drives, memory cards or other devices with similar functions or features.
- 2.7. **Personally Identifiable Information (PII):** Information which can be used to distinguish or trace an individual's identity, such as their name, personal identification number, social security number, biometric records, etc. alone, or when combined with other information which is linked or linkable to a specific individual, such as date and place of birth, employment information, medical information, education information, financial information, etc.
- 2.8. **Secure areas:** Offshore Development Centers (ODC), Data centers, network equipment room, servers' room, other multi-user systems as labs and rooms with sensitive paper-based information, machine containing rooms. No member of the general staff is allowed access, except on special controlled occasions, when they are accompanied at all times by a member of staff. Secure areas may also be subject to restriction on only certain staff members and others when accompanied.
- 2.9. **Board of Directors:** General Director, Vice General Directors.
- 2.10. **Managers:** People who have appointment decisions to the management position, including but not limited to: General Director, Vice General Directors, Directors/ Vice Directors of Software Units (FSU, F CU), Directors/ Vice Directors of Business Units (BU), Heads/ Vice Heads of Business Assurance Departments (BA).
- 2.11. **GitHub Keyword:** are project-specific keywords provided to the company's keyword management tool.
- 2.12. **Company storage:** are devices provided by the company to store data including but not limited to: file-server, FPT SharePoint, PC, Laptop...

Article 3. Duties and responsibilities of functional departments, managers and staffs

- 3.1. Duties and responsibilities of Information security management departments (hereafter called ISM department).
 - 3.1.1. Establish, deploy and manage Company's Information security management system (hereafter called ISMS), assure risk management and take responsibilities of project's ISMS.
 - 3.1.2. Control, audit the compliance of information security management system, provide remedial measures for violation and propose corrective actions.
 - 3.1.3. Organize trainings and create materials of information security management system
 - 3.1.4. Cooperate with other organizations for issues related to ISMS.
 - 3.1.5. Review and update annually this regulation.
- 3.2. Duties and responsibilities of Information Technology departments (hereafter called IT department).
 - 3.2.1. Establish, develop, operate, manage and secure network infrastructure and information systems of Company.
 - 3.2.2. Establish, deploy and report on the surveillance system as well as data access control system, in order to prevent illegal access to computers, information systems and Company network services.
 - 3.2.3. Establish, deploy, report on information systems, network system, data-backup system; record logging and access system, investigate traffic monitor, and protect network system and information systems from any attack.
 - 3.2.4. Provide and deploy technical solutions in information security.
 - 3.2.5. Coordinate with ISM department to deploy Information security policies related to Information Technology equipment, Intranet, servers and Internet connection.
- 3.3. Duties and responsibilities of Administration function
 - 3.3.1. Take charge of physical security and working environment, including electrical system, air conditioners and fire protection.
 - 3.3.2. Manage and report on condition of physical assets and office equipment in Company.
 - 3.3.3. Manage and report on physical access system and access right; camera system and access right.
 - 3.3.4. Manage service providers during their presence in working areas and ensure their compliance of information security.
- 3.4. Duties and responsibilities of Human resource function
 - 3.4.1. Organize Non-disclosure commitment signing and manage the record.
 - 3.4.2. After Non-disclosure commitment signing, request account creation for new employees to access information systems.

- 3.4.3. Request account update and account disabling, once the employees end, cancel or change their labor contracts or their work position.
- 3.4.4. Maintain and review the list of Company's staff account list.
- 3.5. Duties and responsibilities of Recruitment and Training function
 - 3.5.1. Organize Information security training for Staff.
- 3.6. Duties and responsibilities of Quality Assurance function
 - 3.6.1. Do internal audit and control the compliance of information security requirements of projects.
 - 3.6.2. List important projects; collaborate with ISM department to review information security requirements of the projects.
- 3.7. Duties and responsibilities of Unit managers/Business Unit Lead (BUL)/FSoft Unit Lead (FSUL).
 - 3.7.1. Estimate risk before approving special request on the use of information, assets, information access right and information systems access right.
 - 3.7.2. Train; raise staff's awareness of Information security in their Unit.
 - 3.7.3. Take the highest responsibilities of Information security in the Unit they manage, ensure that staff comply with their responsibilities set out in this Regulation.
 - 3.7.4. Coordinate with ISM department to resolve any problem, if any.
- 3.8. Duties and responsibilities of the Information Security Management System (ISMS) Manager at the Unit/FSU
 - 3.8.1. Primarily responsible for organizing and implementing information security (IS) programs at the unit as required by the ISM Department.
 - 3.8.2. Responsible for reporting the results of ISMS program implementation, violations, incidents and security risks to the FSUL/ISM Department.
 - 3.8.3. Act as a bridge between the Unit/FSUL and the ISM Department, coordinating with the ISM Department to address information security issues/incidents.
 - 3.8.4. Monitors compliance within the Unit/FSUL to promptly identify and remediate nonconformities.
- 3.9. Duties and responsibilities of Staff
 - 3.9.1. Understand Information security requirements specified in the documents of ISMS, such as: Information security policies, Regulations, Process description, Job description, Work instructions, Templates and Customer supplied documents.
 - 3.9.2. Be fully aware of and follow these above requirements.

Karan.Gajjar 2025-12-16 05:23:06

CHAPTER II. INFORMATION SECURITY REGULATION

Article 4. Usage of confidential information

- 4.1 Use and disclose confidential information to those who need for work purposes only.
- 4.2 Do not share any confidential information, which the staff can get officially or unofficially to third parties.
- 4.3 Do not use any confidential information for personal purposes (for job application or for sharing with friends or relatives).
- 4.4 Limit collection of personally identifiable information to the minimum necessary to accomplish the work purposes. Do not disclose personally identifiable information of customers, partners or staff to outside parties or to those who are not related to work without permission of authorized person of Company.
- 4.5 Do not upload or store Company's confidential information into any public or personal website or web storage.
- 4.6 Do not upload or store Customer's confidential information into any Internet public or personal include but is not necessarily limited to: Google Drive, GitHub...
PM provides GitHub keywords when the projects open, close and periodically every month to the Information Security Management Department to conduct scanning to identify violation related to uploading and storing Customer's confidential information (*Further information can be found in the Process_Github monitoring*).
- 4.7 Store confidential information in Company storage.
- 4.8 When a project is closed, store project-related information into project's fileservers or storage systems; do not store into computers or mobile devices.
- 4.9 Project-related information shall be deleted from computers, emails and other storages, based on the requirements of Company or project authorized person.
- 4.10 The Company has full rights to use, access to information, data, computers, information systems, networks, applications, software, email, websites and data related to the workplace, area working area of the Company. Accordingly, all employees consent to such collection, access, use and monitoring.

Article 5. Bringing information storage/processing asset, confidential information out of working areas

- 5.1 All information storage and processing assets (including assets belonging to the Company and its Clients) taken outside the company shall be configured in accordance with the company's security standards and receive prior approval from an authorized person and the Information Security Department.
- 5.2 Shall have proper encryption and protection when taking any Company's or customer's confidential information outside.

Article 6. Teleworking and mobile devices

Staff shall comply to this policy:

- 6.1 Only teleworking site or working at home with authorized person's permission. The staff who works from home or teleworking shall have the responsibility to protect information security.
- 6.2 Always follow Company IT department's instruction of regulations on mobile devices, remote connection to Company information systems. It is strictly forbidden to set up a remote connection from a computer at home to the Company without permission from the IT department control.
- 6.3 The following teleworking (including travel, public surroundings) arrangements exist:
 - (i) Teleworking activities are formally managed, controlled and only authorized if suitable security arrangements and security controls that comply with relevant security policies and organizational requirements are in place;
 - (ii) The communications security requirements are addressed and take into account the need for remote access to the organization's internal systems, the sensitivity of the information

that will be accessed and pass over the communication link and the sensitivity of the internal system;

- (iii) The use of home networks and requirements/restrictions on the configuration of wireless network services including encryption (AES WPA2 at a minimum) are addressed;
- (iv) Antivirus protection, operating system and application patching, and firewall requirements consistent with corporate policy are addressed;
- (v) Revocation of authority and access rights and the return of equipment when the teleworking activities are terminated are addressed;
- (vi) Verifiable unique IDs are required for all teleworkers accessing the organization's network via a remote connection;
- (vii) The connection between the organization and the teleworker's location is secured via an encrypted channel;
- (viii) The organization maintains ownership over the assets used by the teleworker in order to achieve the requirements of this control.

Article 7. Non-disclosure commitments and trainings

- 7.1 Staff shall sign and follow Non-disclosure commitment along with his or her labor contract.
- 7.2 Staff may sign and follow Non-disclosure commitment with customer as customer's security requirements.
- 7.3 Before signing labor contract, staff shall attend Company information security trainings and other training courses such as manager training courses, project manager training courses, software developer training courses, trainings for onsite purposes, trainings for business assurance departments, training for Offshore Development Center (ODC), specific training courses for requirements of contracts or projects such as personal information protection, secure coding, secure testing.
- 7.4 Staff shall participate in Company's ISMS refresh training. Depending on the urgency of updating ISMS, the Board of Directors may decide the frequency of ISMS training, but at least 1 time per year.
- 7.5 When hiring personnel from the vendors or partners, Business Unit managers shall be responsible for Non-disclosure commitment and information security trainings for hired personnel.
- 7.6 Staff shall follow work regulation, information security regulation at customer's site.
- 7.7 The access to Company's information, data, computers, information systems, networks applications, software, email, websites and working areas, is monitored and logged by Company. All staff consent to such monitoring and logging.

Article 8. Personal owned device usage for work purposes

- 8.1 Do not use personal owned devices (mobile devices, computers and network devices) to directly connect to the FPT Software's internal network or customer systems for work purposes without authorized person's permission. When it is essential to use those devices, it is required for the staff to have approval from the authorized persons.
- 8.2 Personal owned devices that connect to Company's information systems shall be checked, tested and installed proper anti-virus and endpoint control software by Company's IT department.
- 8.3 Company shall define workforce members roles and responsibilities in the data backup process are identified and communicated to the workforce; in particular, Bring Your Own Device (BYOD) users are required to perform backups of organizational and/or client data on their devices.

Article 9. Account and password management

- 9.1 Company accounts shall be unique not generic or common, individually identified and shall only be used by the person to whom it is assigned. Accounts shall be updated with access rights as soon as staff change positions and responsibilities.
- 9.2 The list of Company staff, contractors, vendors, business partners, etc. who have access to Company's sensitive information is maintained and reviewed regular basis at least one a year.

- 9.3. Staff shall use your Company account without administrator access for your general day to day activities (include Internet and e-mail use) and use a separate local account with administrator access for high privilege activities.
- 9.4. Do not lend others your Company account to access Company's information systems or disclose personal password.
- 9.5. Do not lend others your customer's or third party's account or disclose these passwords to access customer's or third party's information systems.
- 9.6. Do not use or access Company's information systems by others' accounts.
- 9.7. Do not use or access customer's or third party's information systems by others' accounts.
- 9.8. Always follow Company's policy of password creation and password change. Personal password shall be confidential, which is not too simple to be guessed.
- 9.9. Always follow customer's or third party's regulation of password creation and password change when account and password are provided by customer or third party.
- 9.10. Do not search or seek others' passwords.
- 9.11. Default privileged accounts (root, administrator,...) shall not be used for operational activities. These accounts shall have their passwords changed periodically in accordance with regulations and shall be managed strictly, unnecessary system accounts are removed, disabled, or otherwise secured.
- 9.12. To use privileged accounts, accounts have been appropriately reviewed and need to sign a commitment.
- 9.13. Company shall ensure that account managers are notified when users' access rights change (e.g., termination, change in position) and modify the user's account accordingly.

Article 10. Entrance and exit at working areas

- 10.1. Each staff is provided a physical access card with his or her identity photo on it for entrance purpose. The physical access card shall be preserved. Do not lend your card, borrow or swipe an access card on behalf of others to enter working areas or restricted areas. (*Further information can be found in the Standard_Physical and Environmental Security*).
- 10.2. Always wear access card at Company's premises.
- 10.3. Inform to Administration department if access card is lost or omitted within two hours and get temporary backup access card from Administration department. Staff has to return temporary cards to the Administration department within 2 working days. Card administrator who lends temporary backup card has to record lending time and receiving time.
- 10.4. Comply with security signs, safety and office signs at Company's premises. There are secure areas, ODC, where are restricted for only authorized persons. Do not borrow entrance cards or enter these areas without an authorized persons' permission.
- 10.5. Persons in charge from Administration department shall set up visitor entry log books for secure areas where applied specific physical access cards.

Article 11. Usage of cameras and recording devices

- 11.1. Do not use cameras, recorders include but do not limit: cameras, camcorders, recorders, cell phones or devices equipped with cameras, recorders or other devices with similar functions or features at restricted areas with no camera signs, no cellphone signs, no video signs such as: secure areas, ODC, working areas with customer's information and logo at Company's premises or customer site.
- 11.2. Obtain the consent of authorized person when photographing, recording or video recording at restricted areas mentioned in section 11.1.

Article 12. Usage of printers, paper shredders

- 12.1. Printers shall be installed printer log and granted only to authorized staff.
- 12.2. Do not use the Company's printers for any unrelated work purposes.
- 12.3. When it is necessary to destroy confidential documents, always use paper shredders.

Article 13. Usage of fax machines

- 13.1 Do not fax any documents or other materials without an authorized person's permission.
- 13.2 Do not fax any confidential documents.

Article 14. Preservation of hard copy documents and records

- 14.1 Do not leave any confidential documents at public places such as printers; photocopy machines, meeting rooms, laboratories, desks and unlocked cabinets (*Further information can be found in the Standard_Physical and Environmental Security*).
- 14.2 Hard copies of confidential documents shall be classified, placed and preserved in locked cabinets, out of unauthorized people's reach.

Article 15. Information and document transfer

- 15.1 Confidential information and documents shall be transferred only by reliable and secure transport agents, except for emergency case. Document content and receiving time shall be confirmed to the recipients (*Further information can be found in the Standard_Physical and Environmental Security*).
- 15.2 During the information transfer process, always keep devices which contain confidential information along with proper preservation methods.
- 15.3 Company shall perform formally addresses multiple safeguards before allowing the use of information systems for information exchange.
- 15.4 Confidential information sent through any electronic means needs to be encrypted documents and/or zip files with password. Decryption key shall be sent by another email or other means like phone, messenger.

Article 16. Usage of computers and other technology devices

Company shall:

- 16.1 Only use Company standard computers and other technology devices for work purposes and strictly follow Company's regulation of device installation, usage and safeguard.
- 16.2 Do not remove computers or technology device components, request IT department if installation or reparation is needed.
- 16.3 Do not use generic names that cannot be identified for computers and servers. Follow naming convention for computers and servers.
- 16.4 Set up a five-minute automatic screensaver. Always lock the computer before leaving your desk or work area.
- 16.5 Turn off computers and other devices before leaving the office. Register to Administration department and other related department if overnight usage of computers and devices is needed.
- 16.6 Do not share computers' local storage drives, files and folders over LAN/ Wi-Fi or using software.
- 16.7 Do not share the same computer with others.
- 16.8 Every unit shall appoint a manager to manage public computers and devices.
- 16.9 Based on the data classification level, registers media prior to use, places reasonable restrictions on how such media are used, and provides an appropriate level of physical and logical protection for the management of removable media and laptops including:
 - i. Restrictions on the type(s) of media, and usages thereof to maintain security;
 - ii. Registration of certain type(s) of media including laptops. Media containing covered information is physically stored and its data encrypted in accordance with the organization's data protection and privacy policy on the use of cryptographic controls until the media are destroyed or sanitized and commensurate with the confidentiality and integrity requirements for its data classification level.

Article 17. Usage of software/extension

- 17.1 Use authorized software in the Company's whitelist only.

The installation or use of any software not included in the company's whitelist or blacklist, as well as any browser extensions, is strictly prohibited without prior approval and assessment from the Manager and the Information Security department.

- 17.2. Unlisted software or blacklist is strictly forbidden. Do not use any scanning, monitoring, attack, hacking software, bypass networks, or disable unauthorized default settings in office.
- 17.3. Personal or individual-use licenses are prohibited for any company-related activities. This includes software, fonts, images, and other copyrighted materials. All company work shall utilize resources with appropriate commercial licenses obtained by the company or provided by customers.
- 17.4. Only Artificial Intelligence (AI) tools listed in the company's approved usage catalog may be used. These tools shall be controlled and comply with the regulations on AI tool usage (*Further information can be found in Regulation_Acceptable Use for AI*).

Article 18. Usage of mobile devices, network devices and peripherals

- 18.1. Mobile devices that connect to Company's network system and to other technology services shall follow Company's information security policy and IT department's instruction during registration; protection, such as: password creation, encryption, key cable locks; usage and cancelation.
- 18.2. Using devices with network connectivity functions or creating or sharing WiFi to other devices for accessing Company network or internet is strictly forbidden.
- 18.3. Other network devices shall be registered to Company, tested and managed by IT department, if any.

Article 19. Usage of Company emails

- 19.1. Email systems are considered to be the Company's property which are provided for serving operational and administrative purposes in connection with the business (*Further information can be found in Standard_Email*).
- 19.2. Use Company email or authorized emails for work purposes only, do not use other email systems at the office.
- 19.3. Free well-known emails (such as: Gmail, Yahoo, Hotmail...) are prohibited to send, receive and use.
- 19.4. Always check email address (To, Cc, Bcc), email subject, email content, attached files and signature before sending an email. Scan virus before sending emails.
- 19.5. Use the latest signature provided by Corporate Communications department for sending emails, replying to emails and forwarding emails.
- 19.6. Do not use Company's email for testing; do not install email servers. If needed, Managers and IT permission is required.
- 19.7. Do not use accounts of other people, lend or borrow email accounts.
- 19.8. Do not disguise identity, and forge emails, crack passwords, hack, attack, or mass mailing to Company's or other email systems.
- 19.9. Do not use email to send or forward materials that could be construed as offensive to a person or organization or against the national traditions and customs, information that violates national security regulations.
- 19.10. Do not forward messages to others or mailing lists, without the permission of the originator.
- 19.11. Do not forward or auto-forward Company's emails to other email systems.
- 19.12. Do not use Company's emails to register to any forums or social websites.
- 19.13. Do not send confidential information via email. If necessary, you shall have the permission from authorized person and properly encrypt documents or zip files with password. Decryption key shall be sent by another email or other means like phone, messenger.
- 19.14. Do not open phishing emails or emails that look suspicious with signs such as domain name is not from a trusted company; emails do not specify a specific recipient; emails have spelling and grammatical errors.
- 19.15. Do not click on links in phishing or suspicious emails; never reply to phishing or suspicious emails or provide personal information, username, and password.

- 19.16. Report to IT and ISM department when receiving phishing or suspicious emails.
- 19.17. Users are prohibited from abuse of email usage, include but is not necessarily limited to: using email to operate a business, conducting an external job search, soliciting money for personal gain, campaigning for political issues, or promoting funds for a religious purpose or any other activity of a similar nature.
- 19.18. Do register to IT department before using any mobile devices to access Company email system and follow IT department's instruction of password creation and data encryption.
- 19.19. Do hand-over your mailing lists and special emails, if any, to the person in charge when changing work position.
- 19.20. Identify account types (individual, shared/group), conditions for group and role membership are established, and, if used, ensure shared/group account credentials are modified when users are removed from the group.

Article 20. Usage of Intranet, information systems, servers and Internet

Company shall:

- 20.1. The access to information system, applications, functions, data is provided, authorized and controlled based on "roles and responsibilities", "need to know", "need to use", "need to work" basis. Access the information, which is approved by authorized person of Company or customer only.
- 20.2. Authorized persons who grant access right to information system or data shall be responsible for carrying out the risk assessment and re-checking the implementation to ensure that the access right is for the right person and right scope.
- 20.3. Do not use Intranet, information systems, servers and the Internet for non-work purposes.
- 20.4. All servers, which provide Internet services, shall be tested and managed by IT department.
- 20.5. Do not install servers that provide services such as Web, FTP, SVN, Proxy, Firewall, DC, DNS and DHCP without authorized person's permission.
- 20.6. Do not configure the network, do not set up Internet for computers that are in the internal network without an authorized person's permission.
- 20.7. Do not access websites that are unrelated to work purposes; do not use gateway to bypass Company's or customer's proxy.
- 20.8. Do not use online tools or public websites to translate documents containing Company's confidential information. Only use tools or websites that are developed, supplied or assigned to translate documents containing confidential information of the Company.
- 20.9. Do not abuse Company's network infrastructure, devices and other resources for non-work purposes include but not limit to operate a business, conducting an external job search, soliciting money for personal gain, campaigning for political issues, or promoting funds for a religious purpose or any other activity of a similar nature.
- 20.10. Do not hack or attack Company's network or server; or abuse Company's network infrastructure, devices and other resources to hack or attack external network or server.
- 20.11. The use of cloud computing services for business purposes shall be approved by the IT Head (*Further information can be found in the Standard_Cloud Computing*).
- 20.12. Access rights to applications and application functions are limited to the minimum necessary using menus.
- 20.13. Identify account type (individual, system, application, guest/anonymous, emergency and temporary), conditions for group and role membership are established, and, if used, account credentials are modified when users are removed from the group.
- 20.14. Review and reallocated user access rights when moving from one employment or workforce member arrangement to another within Company.

Article 21. Antivirus and system update

- 21.1. Computers and other information technology devices shall be installed and updated the latest version of Antivirus software and scanned virus regularly, following IT department's instruction. Do not turn this software off or remove it.

- 21.2. Computers and other information technology devices shall be installed automatically system and software updates. Check these processes and report to the IT department for any errors.
- 21.3. Disconnect Internet connection as soon as the computer is detected with virus, report to IT department for solution.
- 21.4. Do not spread malicious programs (such as viruses, worms, trojans, bomb letters ...) from the computer and/or equipment of Company or into the network and/or servers of Company.

Article 22. Usage of customer's assets

- 22.1. Customer supplied assets (infrastructure, information system, application/software, network connection, server, Internet, device, account/password, email...) are considered to be customer properties which are provided for serve operational and administrative purposes in connection with the business.
- 22.2. Follow customer's policy or work instruction on the usage of customer's assets when you are provided.
- 22.3. Follow Company Information Security Regulation for customer's assets if customer does not provide detailed requirement or guidance.
- 22.4. Use and preserve customer's device, account/password, email, access right...which are assigned to you based on "need to work" principle.
- 22.5. Do not abuse customer's assets for non-work purposes include but not limit to use for wrong intended propose, operate a business, conducting an external job search, soliciting money for personal gain, campaigning for political issues, or promoting funds for a religious purpose or any other activity of a similar nature.
- 22.6. Do not hack or attack customer's network or server; or abuse customer supplied assets to hack or attack external network or server.
- 22.7. Hand-over customer's assets, if any, to person in charge when changing work position.

Article 23. Use of social media

- 23.1 Do not post, upload, share or disclose confidential information or photos of the Company or customer when participating in blogging, participating in social media.
- 23.2 Customer's personally identifiable information or their photos shall not be made available on social media.
- 23.3 Do not post, upload, share or disclose any photos of customer sites or Company's ODC, restricted areas, no cameras sign areas on social media.
- 23.4 Do not post, upload, share or disclose the information of working schedule, working location, business contents of your own or your managers on social media.

Article 24. Information security incident management

- 24.1. Immediately inform Supervisors and Head of ISM department within 2 hours after detecting information security incidents (*Further information can be found in the Standard_Information Security Incident Management*).
- 24.2. Do follow customer's requirements of information security incident management if there are specific or predefined requirements with customer.
- 24.3. Cooperate with Company and/or customer to resolve information security incidents, if required.

CHAPTER III. HANDLING OF INFORMATION SECURITY VIOLATION

Article 25. Basis of the handling information security violation

Determining forms of information security violation handling shall depend on the following:

- 25.1 Violation behaviors;
- 25.2 Level of risk, threat: information leak and loss;
- 25.3 Actual loss: physical loss and reputation loss;
- 25.4 Types of violation: intentional or unintentional violation.

Article 26. Forms of handling information security violation

The staff that violates Information security regulation shall be penalized one or all of these following disciplines:

- 26.1 Bonus deductions (see Chapter V. Appendix of bonus deductions).
- 26.2 Participating in the ISMS re-training courses.
- 26.3 Violation shall be one of the factors to assess the level of task completion.
- 26.4 Compensation for damage under the laws.
- 26.5 Staff violations may also be considered according to disciplined behaviors and disciplined forms that are defined in Company's Labor regulations.

Article 27. Handling of information security violation

- 27.1 The ISM department is responsible for reporting to the managers who are in charge or to the CEO for remedial measures.
- 27.2 Handling process of information security violation is in compliance with labor discipline defined in Company's Labor regulations.

CHAPTER IV. IMPLEMENTATION PROVISIONS

Article 28. Implementation responsibility

- 28.1 This Information Security Regulation is effective from the date of signing, replacing all previous regulations on Information Security.
- 28.2 ISM department is responsible for creating procedures and guidelines, supervising, testing and evaluating the deployment of this regulation in every Company business unit.
- 28.3 Directors, managers of business branches, representative offices, subsidiary companies and other units are responsible for organizing and implementing this regulation.

Article 29. Amendment and supplementation

- 29.1 This regulation shall be adjusted, amended or supplemented, depending on Company's actual situation of business and on amended, supplemented content of the Labor law.
- 29.2 Amendment and supplementation of this regulation shall be consulted by Company's Legal Risk and Compliance department as well as Human Resources department and be approved by CEO.

HaNoi, May 29th, 2025

P.P. CHIEF EXECUTIVE OFFICER

DEPUTY GENERAL MANAGER



APPENDIX OF BONUS DEDUCTIONS

Notes on the deduction levels for violations listed from Article 4 to Article 24 as per the table below:

- I: The first-time violation
- II: Repeat a violation from the 2nd time

Additionally, for the following cases/individuals:

- The violators are managers.
- Managers of Business Units or Departments, Project Manager those occurred incidents.
- Managers (including Business Units or Departments and Project Manager) do not pay attention enough in managing staff and/ or do not ensure that their staff are trained or adhere to the company's regulations leading to information security violations.

The following deductions shall be applied based on the severity of the incident:

- Major Incident: Deduct at least 01 level higher than the level of the violating employee, including the following cases:
 - Violation relates to the detection of customers and/ or the involvement of the Board of Directors.
 - Violation causes serious harm to the Company, with the potential to affect the Company's interests, reputation, or legal standing.
- Internal Incident – Limited to internal impacts: A bonus deduction applied is equal to the violating employee.

In cases where an employee incurs the highest bonus deduction (20 million VND or more), the Information Security Department will evaluate the situation and propose an appropriate deduction for the manager. The final deduction amount will be reviewed and decided during the labor disciplinary meeting.

Employees who violate the Information regulations will be applied to the bonus deduction as table below:

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000 or more
Article 4. Usage of confidential information					
1	Bring confidential information out of Company; disclose confidential information to third parties, which causes damage to Company's image and reputation.				I
2	Send confidential information to wrong customers.				II
3	Use confidential information or information assets for non-work purposes.	I	I	I	II

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000
4	Do not limit the collection of personally identifiable information to the minimum necessary to accomplish the work purposes.				
5	Disclose personally identifiable information of customers, partners or staff to outside parties or to those who is not related to work without permission of authorized person of Company.				
6	Upload or store Company's confidential information into public or personal website or web storage.				
7	Do not store confidential information into company storage.				
8	Do not remove work-related or project-related information in computer or mobile devices when project is closed.				
9	After customer's request, do not remove project information from computers, emails and other storages when the project is closed.				
10	Upload or store Customer's confidential information into any Internet public or personal include but is not necessarily limited to: Google Drive, Github...				
11	Do not provide GitHub keywords when the projects open, close and periodically every month.				
Article 5. Bringing information storage/processing asset, confidential information out of working areas					
12	Bring Company's storage/processing asset or confidential information out of working areas without authorized person's permission.				
13	Bring customer's storage/processing asset or confidential information out of working areas without authorized person's permission.				
14	Bring Company's confidential information or storage/processing assets out of working areas without a proper encryption and protection.				
15	Bring customer's confidential information or storage/processing assets out of working areas without a proper encryption and protection.				
Article 6. Teleworking and mobile devices					
16	Teleworking and working from home without authorized person's permission.				
17	Do not protect information security at teleworking site or when working from home.				

(*) Based on the extent and severity of damage caused by the violations, the sincere attitude or positive remedial actions of violator.					
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000 or more
4	Do not limit the collection of personally identifiable information to the minimum necessary to accomplish the work purposes.				
5	Disclose personally identifiable information of customers, partners or staff to outside parties or to those who is not related to work without permission of authorized person of Company.				
6	Upload or store Company's confidential information into public or personal website or web storage.				
7	Do not store confidential information into company storage.				
8	Do not remove work-related or project-related information in computer or mobile devices when project is closed.				
9	After customer's request, do not remove project information from computers, emails and other storages when the project is closed.				
10	Upload or store Customer's confidential information into any Internet public or personal include but is not necessarily limited to: Google Drive, Github...				
11	Do not provide GitHub keywords when the projects open, close and periodically every month.				

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000 or more
18	Do not follow Company's requirements of remote connection installation and usage to Company information systems Set up a remote connection from a computer at home to the Company without permission from the IT department's control				
	Article 7. Non-disclosure commitment and trainings				
19	Do not sign Non-disclosure commitment along with his or her labor contract.				
20	Do not sign Non-disclosure commitment with customer as customer's security requirements.				
21	Absent from Information security trainings, other annual training courses, manager training courses, project manager training courses, software developer training courses, trainings for onsite purposes, trainings business assurance departments, trainings for Offshore Development Center, specific training courses for requirements of contracts or projects such as personal information protection, secure coding, secure testing.				
22	When hiring personnel from the vendors or partners, Business Unit managers do not have Non-disclosure commitment and information security training for hired personnel.				
23	Do not follow work regulation and information security regulation at customer's sites.				
	Article 8. Personal owned device usage for work purposes				
24	Use personal owned devices (mobile devices, computers and network devices) for work purposes without authorized person's permission.				
25	Use personal owned devices that connect to Company's information systems without IT department's permission.				
	Article 9. Account and Password management				
26	Do not follow the Company's regulation of password creation and password change. Do not keep your password confidential, or it is too simple to be guessed.				
27	Do not follow customer's or third party's regulation of password creation and password change when account and password are provided by customer or third party.				

Karantina Software 05.23.06

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000
28	Use default privileged accounts for operational activities. It is not changed the passwords periodically in accordance with regulations and not strictly managed				
29	Lend others Company's accounts to access confidential information systems.				
30	Lend others your account or disclose these passwords to access customer's or third party's information systems				
31	Use or access Company' information systems by other's account.				
32	Use or access customer's or third party's information systems by others' accounts.				
33	Search or seek others' passwords.				
Article 10. Entrance and exit at working areas					
34	Using another person's access card or allowing others to use your own, including swiping or requesting card swipes on behalf of others, to access the workplace (bonus deductions will multiply by the number of violations)				
35	Open access doors for other Company staff or non-staff or swipe an access card on behalf of others to enter working areas or restricted areas				
36	Do not wear access card at Company's premises.				
37	Do not inform to administration department within two hours since personal access card is lost or omitted.				
38	Do not get a temporary backup access card from the administration department when access card is lost or omitted. Or do not return temporary card to administration department within 7 working days				
39	Card administrator lends temporary backup card without recording card lending time and receiving time.				
40	Enter secure areas without an authorized person's permission. Do not comply with security signs, safety and office signs at Company's premises and customer site.				

No.	Violations	Bonus deductions level			
		From 500.00 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000 or more
41	Administrators do not set up entry logbooks for secure areas where applied specific physical access cards.				
	Article 11. Usage of cameras and recording devices				
42	Use cameras, recorders include but do not limit: cameras, camcorders, recorders, cell phones or devices equipped with cameras, recorders or other devices with similar functions or features at restricted areas with no camera signs, no cellphone signs, no video signs such as: secure areas, ODC, working areas with customer's information and logo at Company's premises or customer site.				
43	Do not obtain the consent of authorized person when photographing, recording or video recording at restricted areas mentioned in section 11.1				
	Article 12. Usage of printers, paper shredders				
44	Do not install printer log, do not appoint printing right to only specific people or groups.				
45	Use Company's printers for unrelated work purposes.				
46	Do not use paper shredders, when it is necessary to destroy confidential documents.				
	Article 13. Usage of fax machines				
47	Fax documents or other materials without authorized person's permission.				
48	Transfer confidential information by fax machines.				
	Article 14. Preservation of hard copy documents and records				
49	Leave confidential documents or materials in public places such as printers, photocopy machines, meeting rooms, labs, desks and unlocked cabinets.				
50	Do not classify, place and preserve hard copies of confidential documents in locked cabinets, out of unauthorized people's reach.				
	Article 15. Information and document transfer				
51	Do not get confidential information and documents transferred by reliable transport agents, except urgencies.				

(*) Based on the extent and severity of damage caused by the violations, the sincere attitude or positive remedial actions of violator.

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000
52	Loss or disclosure of confidential information due to careless information transfer.	—	—	—	
53	Send confidential information without encrypted documents and/or zip files with password.	—	—	—	
	Article 16. Usage of computers and other technology devices				
54	Use Company's computers and other technology devices for non-work purposes.	—	—	—	
55	Remove computer or technology device components without authorized person's permission.	—	—	—	
56	Use generic name that cannot be identified for computers and servers. Or do not follow naming convention for computers and servers.	—	—	—	
57	Do not set up five-minute automatic screensaver.	—	—	—	
58	Do not lock computer screens before leaving desk or work areas.	—	—	—	
59	Do not shut down computers and turn off other devices before leaving office, except the case when the computers are required for overnight work.	—	—	—	
60	Use computers overnight for work purposes without registering to admin department and related departments.	—	—	—	
61	Share computers' local storage drives, files and folders over LAN/Wi-Fi or using software.	—	—	—	
62	Share computer or use other's computers.	—	—	—	
63	Lose laptops, devices and other assets provided by Company or personal owned which contain confidential information, customer's information or project-related information.	—	—	—	
64	Managers of departments or business units who do not appoint a member to manage public computers and devices of their units.	—	—	—	
	Article 17. Usage of software				
65	Download, crack, use or store unlicensed software or un-authorized software.	—	—	—	
66	The installation or use of any software not included in the company's whitelist or blacklist, as well as any browser extensions without prior approval and assessment from Manager and the Information Security department that could pose security incident/risk.	—	—	—	

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000
67	Download, crack, use or store unlicensed software, which causes virus infection to Company's internal network, documents, sent to customers or which affects project schedule.				
68	Use forbidden software, software in Blacklist. Use or test any scanning, monitoring, attack, hacking spy software, bypass networks, or disable unauthorized default settings at office.				
69	Use the AI tools not listed in the company's approved usage catalog. Failure to control and comply with regulations when using AI tools, resulting in incidents or significant risks to information security				
70	Use inappropriate licenses causes security incident or compliance issues.				
Article 18. Usage of mobile devices, network devices and peripherals					
71	Use mobile devices connected to Company's network system and other technology services, which do not meet Company's requirements of registration, installation, usage and security (password or encryption).				
72	Use devices with network connectivity functions, create or share WiFi to other devices for accessing Company network or internet.				
73	Use network devices, which are not configured and managed by IT department.				
Article 19. Usage of Company emails					
74	Use Company emails or authorized emails for non-work purposes.				
75	Use free emails, personal emails or other email systems, except emails provided by customers.				
76	Send emails to wrong recipients (To, Cc, Bcc), wrong email title, wrong email content, wrong attached files or there is virus in the emails.				
77	Do not use the latest signature provided by Corporate Communications department for sending emails, replying to emails and forwarding emails.				
78	Use Company emails for testing. Set up email server without the permission of IT department.				
79	Use other's emails account, lend or borrow email account.				
80	Disguise identity, forge emails, crack password, hack, attack to Company emails or other email systems.				

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000 or more
81	Spam emails to Company emails or other email systems.				
82	Send or forward materials that an individual or organization or against the national traditions and customs, information that violates national security regulations.	-	-		
83	Forward emails to individuals or mail lists that are not approved by the original sender.				
84	Forward or auto-forward Company's emails to other email system.	-	-		
85	Use Company's emails to register to forums or social websites.	-	-		
86	Send confidential information via emails without Z/EP/ encryption.	-	-		
87	Open or click on links in phishing or suspicious emails; reply to phishing or suspicious emails; or provide personal information, username, and password. Do not report to IT and ISM department when receiving phishing or suspicious emails	-	-		
88	Abuse of email usage includes but is not necessarily limited to: using email to operate a business, conducting an external job search, soliciting money for personal gain, campaigning for political issues, or promoting funds for a religious purpose or any other activity of a simila nature.	-	-		
89	Do not register to IT department before using any mobile devices to access Company email system and follow IT department's instruction of password creation and data encryption	-	-		
90	Do not hand-over mailing lists and special emails, if any, to person in charge when changing work position.	-	-		
Article 20. Usage of Intranet, information systems, servers and Internet					
91	Access websites that are forbidden, unauthorized and unrelated to work purposes.	-	-		
92	Authorized persons who grant access right to information system or data do not carrying out the risk assessment, and do not re-checking the implementation that led to the violate of access right and "need to work" basis	-	-		
93	Use Intranet, information systems, servers and the Internet for non-work purposes	-	-		

(*) Based on the extent and severity of damage caused by the violations, the sincere attitude or positive remedial actions of violator.

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000 or more
94	Use servers, which provide Internet service that are not tested and managed by IT department.				
95	Install servers that provide services such as Web, FTP, SVN, Proxy, Firewall, DC, DNS and DHCP without authorized persons permission.				
96	Configure network or set up Internet for computers that are in internal network without authorized person's permission.				
97	Access websites that are unrelated to work purposes. Use proxy gateway to bypass Company's or customer's proxy.				
98	Use online tools, public websites or unauthorized tools/websites to translate or convert documents containing confidential information of the Company.				
99	Abuse Company's infrastructure, devices and other resources for non-work purposes include but not limit to: operate a business, conducting an external job search, soliciting money for personal gain, campaigning for political issues, or promoting funds for a religious purpose or any other activity of a similar nature				
100	Hack or attack Company's network or server; or abuse Company's network infrastructure, devices and other resources to hack or attack external network or server	-	-	-	-
101	Use cloud computing services without the review or approval of IT department.				
Article 21. Antivirus and system update					
102	Download; clone virus-infected information or files from the Internet or from other computers and devices.				
103	Do not install and update the latest version of Antivirus software on computers and other technology devices.				
104	Spread malicious programs into the network and servers (such as viruses, worms, trojans, bomb letters...).				
105	Turn off or remove antivirus software, antivirus update or regular antivirus scan.				
106	Do not check installed system and software automatic updates and do not report to IT department for any errors.				
107	Do not disconnect Internet connection as soon as computers are detected with virus, do not report to IT department for solution.				

No.	Violations	Bonus deductions level			
		From 500.000 to 2.000.000	From 2.000.000 to 6.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000
Article 22. Usage of customer's assets					
108	Do not follow the customer's policy or work instruction on the management of customer's assets when you are provided. Do not use customer's assets with intended purpose.			I	II
109	Do not preserve customer's device, account/password, email, access right... that are assigned to you based on "need to work" principle.		I		II
110	Abuse customer's assets for non-work purposes include but not limit to: operate a business, conducting an external job search, soliciting money for personal gain, campaigning for political issues, or promoting funds for a religious purpose or any other activity of a similar nature.		I		II
111	Hack or attack customer's network or server; or abuse customer's assets to hack or attack external network or server.			I	
112	Do not hand-over customer's assets, if any, to person in charge when changing work position		I		II
113	Lose customer's assets.			I	II
Article 23. Use of social media					
114	Post, upload, share or disclose confidential information or photo of Company or customer when participating in blogging, participating in social media.		I		II
115	Post, upload, share or disclosure customer's personally identifiable information or their photos on social media.		I		II
116	Post, upload, share or disclose photos of customer sites, photos of Company's ODC, restricted areas, no cameras sign areas on social media.		I		II
117	Post, upload, share or disclose the information of working schedule, working location, business contents of your own or your managers on social media.		I		II
Article 24. Information security incident management					
118	Do not inform to Supervisors or Head of ISM department, within 2 hours, after detecting of the loss, the theft and unauthorized disclosure of information assets of the Company or information security incidents.			I	II
119	Do not follow customer's requirements of Information security incident management if there are specific or predefined requirements with customer.			I	II

(*) Based on the extent and severity of damage caused by the violations, the sincere attitude or positive remedial actions of violator.

No.	Violations	Bonus deductions level		
		From 500.000 to 2.000.000	From 6.000.000 to 10.000.000	From 10.000.000 to 20.000.000
120	Do not cooperate with Company or customer to resolve information security incidents, if required.	I	II	II

(*) Based on the extent and severity of damage caused by the violations, the sincere attitude or positive remedial actions of violator.				
From 500.000 to 2.000.000	2.000.000 to 6.000.000	6.000.000 to 10.000.000	10.000.000 to 20.000.000	From 20.000.000 or more

RECORD OF CHANGE

No	Effective Date	Version	Change Description	Reason	Reviewer	Approver
1	30-Oct-2017	4.1	- Add secure coding, secure testing training. - Modify the requirements about sharing computers' local storage drives and software.	Need for yearly reviewing and improving policies, documents	TuanPM	
2	15-Nov-2019	4.2	- Add phishing email - Request from LRC department on the management responsibility in information security compliance in section 2.10, 3.7.3, Article 26. Forms of handling violations, add deduction case for manager.			
3	06-Jun-2020	4.3	- Add 3.4 Duties and responsibilities of Human resource function: 3.4.4 Manage the Company's staff account list. 4.9 The Company has full authority to monitor and log the access to Company's information, data, computers, information systems, networks, applications, software, email, websites and working areas. Article 8. Personal owned device usage for work purposes: 8.2 "and endpoint control software" Article 9 Account and password management: 9.1 Accounts must be updated with access rights as soon as staff change positions and responsibilities 9.2 The lists of Company staff, suppliers, business partners who have access to Company's confidential information are maintained and reviewed regular basis at least one a year.	- Working environment and Working Way (WFH) is changed, CDTO and IT Lead Department decide the frequency of ISMS training (section 7.3) - Update Policy that met to the requirement of HITRUST standard (section 7.6, 9.3, 20.1) - Review and innovate document according to annually revision requirement of company	DungNQ7	

			(Other: The order of items in Article 9 are changed)			
			20.1 The access to information system, applications, functions, data is provided, authorized and controlled based on "role-based access"; "need to know", "need to use", "need to work" basis.			
			- Update 7.4 Staff must participate in Company's ISMS refresh training. Depending on the facts of an actual situation, the Board of Directors may decide the frequency of ISMS training, but at least 1 time per year.			
			- Modify Chapter V. Appendix of bonus deduction:			
			The order of items in Article 9 are changed.			
4	28-Apr-2021	4.4	- Additional 4.6: do not upload customer's information to the public internet.	Enhance employee awareness when using customer's information assets	CuongDD	
			- The Bonus deductions level is increased 2 times			
5	22-Jul-2021	4.5			CuongDD	
6	15-Oct-2021	4.6	Update article 16. Usage of computers and other technology devices		CuongDD	
7	01-May-2023	4.7	Document Code: 15/2021/QDh/FSOFT-ISMS_EN 1/ updated "FPT Software" to "Company" as defined in Article 1. 2/ new added: - 6.3; 7.7; 8.3; 9.11; 9.12; 9.13; 15.3; 16.9; 19.20; 20.12; 20.13, 20.14. - 2.11; 2.12; 4.7; 15.4; Violations No. 11; Violations No. 53. 3/ updated: 4.6; 4.7; 10.3; Note of Chapter V. 4/ updated content of Violations: Article 4: no.7, no.11 and Article 15; No 53	HieuLC5 AnhBP UyenNTM DungNQ7	CuongDD	

		5/ general format: corrected grammar & spelling, updated alignment; re-indexed, and table of contents according to the changes. 6/ updated "further information" document using correct naming from QMS. e.g. "Cloud computing standard" to "Standard_Cloud Computing"		
8	30-May-2025	5.0	<p>1/ New added: 3.82/ Update Article 5 (merge 5.2 into 5.1), Article 17, 8.1, 9.11, 10.1 3/ Remove: 17.3, 17.4 (old clauses)</p> <p>4/ Update: APPENDIX OF BONUS DEDUCTIONS</p> <ul style="list-style-type: none"> - The bonus deduction cases shall be applied for Manager based on the severity of the incident - Bonus deduction for managers when employees are fined 20 million VND or more. - 26. Do not keep your password confidential, or it is too simple to be searched: Increase the bonus deduction for the first violation from 500.000 – 2.000.000 to 2.000.000 – 6.000.000 and the second violation from 6.000.000 – 10.000.000 to 10.000.000 – 20.000.000 - 66. Add new bonus deduction case: The installation or use of any software not included in the company's whitelist or blacklist, as well as any browser extensions without prior approval and assessment from Manager and the Information Security department <p>- 69. Add new bonus deduction case: Use and manage AI tools</p> <p>- 70. Add new bonus deduction case: Use inappropriate licenses causes security incident or compliance issues</p>	<p>TungNT2 ChuongTD1</p> <p>- Request regulatory updates from the corporation</p> <p>- Need to clearly define ISMS Manager responsibilities to promote ISMS Manager program</p> <p>- Need to update ISM documents annually</p> <p>- Update and clarify bonus deduction regulations as requested by relevant departments</p> <p>- Clarify some information security regulations and add some new regulations.</p> <p>- 69. Add new bonus deduction case: Use and manage AI tools</p> <p>- 70. Add new bonus deduction case: Use inappropriate licenses causes security incident or compliance issues</p>

		<ul style="list-style-type: none">- Update: 12 to 15, 28, 34, 35, 68- Remove bonus deduction clause (the clause number below is the old clause number):<ul style="list-style-type: none">+ 68. Use peer to peer software, file sharing software or desktop sharing software.+ 69. Use Proxy and Firewall bypass software, website include but do not limit: Tor, Freegate,..
--	--	--