Concept Note for the Revision of Mekong Institute's Operations Manual, Staff Salary Scale and Organization Structure

1. Background

The countries of Cambodia, Lao PDR, Myanmar, Thailand, and Viet Nam (CLMTV) are intricately linked by economic, social, political, cultural, and environmental interdependencies, forming the cohesive Greater Mekong Subregion (GMS). For over two and a half decades, the Mekong Institute (MI) has stood as a vanguard for forging dynamic partnerships and facilitating collaborations within the GMS. MI, jointly owned and governed by the six GMS countries, is an international organization that deepens regional cooperation and integration through capacity development, dialogue, and advocacy for the acceleration of sustainable socioeconomic development and poverty alleviation in the GMS.

Guided by its Strategic Plan 2021-2025, MI is committed to becoming a center of excellence in human resource development, a think tank, and a convener for dialogue and collaboration. To transform this mission into action, MI has been striving to enhance and harness potentials of its current staff and transform into a learning organization built on an upgraded organizational structure that reflects more efficient human resources and operations.

In addition, the findings and recommendations of the Mid-Term Review of MI's Strategic Plan 2021 – 2025 also echoes the same message, calling for the need for MI to attract leading experts and specialists into MI's fold, strengthen the in-house expertise, and recalibrate its organizational structure, taking into account a rapidly changing regional context and the post-pandemic landscape.

2. Rationale

MI's Operations Manual is a guiding document which defines policies and procedures related to human resources management, administration, procurement, and finance. It also serves as a procedural map reflecting all personnel related issues, allowing the Executive Director, Senior Management Team (SMT) and staff to exercise delegated authority effectively and efficiently.

Considered as a living document, the Operations Manual has been periodically revised and updated. In 2015, the revision was made by an external consultant and the revised Operations Manual was implemented from January 1, 2016.[1] In 2020, it was internally reviewed and updated and the revised Operations Manual was implemented from January 1, 2021 until now.

To meet the commitments mapped out in the Strategic Plan, MI sees the need to further revise and update the current Operations Manual, particularly the overall Institutional Organization, Human Resource, General Service, Procurement, Finance, Communications and Knowledge Management and Information Technology. As such, MI hired an external consultant to review and update the current Operations Manual to ensure it remains compliant with changing laws,

[1] The committee members who were appointed appears in Annex I.

regulations and in line with international practices with similar nature to MI. The ultimate goal is to consolidate MI's human resource and enhance internal systems and procedures.

3. Process

To ensure that the Operations Manual remains valid and fits the other organizations' implementation and the internal organization context, a term of reference was drafted and a competitive bidding was undertaken. An external consultant, **Mr. Danny K. Amenigy, and his team**, was contracted to oversee the task of updating and revising the Operations Manual from May – September 2023. His present address is in South Africa.

The committee members consist of:

- Mr. Rithy Buth, Director of Finance and Operations Department
- Mr. Madhurjya Kumar Dutta, Director of Trade and Investment Facilitation Department
- Ms. Phinyada Foytong, Finance Manager
- Ms. Jutamas Thongcharoen, Program Manager
- Ms. Anusara Tanpitak, CKM Manager
- Ms. Than Tha Aung, Senior Program Coordinator
- Ms. Vitchaya Panurak, Human Resource Officer
- Ms. Kanrayanat Yatsom, Procurement Officer

4. Key Revisions

The sections which have been revised appear in the attached file. Below is the summary of key revisions.

4.1 Revised Staff Salary Scale

Purpose: The current salary scale has been revised in an effort to reflect an effective salary range in line with the market pay and is driven by the aim to hire qualified staff and increase staff satisfaction and retention. It is expected to support the organization with productive and highly-qualified staff according to the staff's commitment and expertise.

Report and justification on the MI Salary survey and revision: The SMT have noted with concern the sporadic inflationary trend in Thailand which had brought in its wake a significant erosion of staff salaries. It was also noted that when employees perceive significant disparities in salaries within MI and compared to other analogous organizations, this has led to a sense of unfairness and inequality. The perception that their counterparts in similar roles may be earning more for comparable work leads to low productivity and inertia. MI management, on the other hand, are geared up to retain highly skilled employees. On this basis, the management took the decision to recruit a consulting team to undertake a salary survey for the adjustments of salaries that will align with market conditions and the varied values employees bring to MI. The consultants took into cognizance various indices in undertaking the comprehensive salary survey. The empirical research revealed the following, supporting the need for the survey and adjustments.

Sources: MI's salary scale compared with various sources.

- The consultant's analysis
- The consultant for staff salary survey: The consultant interviewed private sector and international and regional organizations in GMS countries.
- UN Website

Factors: Consultants focus on

- Market rate
- Cost of living index
- Inflation
- Increased job responsibilities

MI has not conducted a staff salary survey since 2014. MI conducted a staff salary survey through an external consultant from June - September 2023.

The detailed Revised Staff Salary Scale is in Annex 2

4.2 Revised Organization Structure

❖ Benefits of Organizational Structure Change
- ✓ Reflect on the five-year strategic plan
- ✓ Refer to the organization's growth (number of projects and funding)
- ✓ A cohesive vision and values
- ✓ Functioning teams

❖ Main current structure maintained with minor revisions
- ✓ An internal audit unit will be established.
- ✓ The Partnership and Resource Mobilization (PRM) Unit has been changed to External Relations & Protocols Unit. Work related to "partnership and resource mobilization" will become an internal mechanism while selected staff will be appointed as Country/Partner Focal Persons
- ✓ All Specialist positions should be recruited based on the projects' needs; the specialist positions will play roles as in-house expertise.
- ✓ Some Manager positions will play roles as senior positions; s/he will expand their responsibilities such as proposals, reporting, project management, and being in charge of the department director when the director position is not in the office.
- ✓ The Procurement Unit will be combined with HR.
- ✓ IT will become a separate unit.

The detailed Revised Staff Salary Scale is in Annex 3

4.3 Revised Operation Manual, Parts

MI revised the overall Institutional Organization, Human Resources, General Service, Procurement, Finance, Communications and Knowledge Management and Information Technology.

The detailed Revised Staff Salary Scale is in Annex 4

5 Governing Board Action

MI kindly requests our Governing Board (GB) members to consider and approve the aforementioned changes and updates. Upon the approval from the GB, particularly on the revised staff salary scale, MI Organization Structure and Others and MI shall proceed with the following actions:

5.1 Revised Staff Salary Scale

- Put positions from the organization structure in the salary scale description according to the roles and responsibilities

- If the current staff does not reach the new salary scale, the staff will be at Level 1
- If the current staff reaches the new salary scale, SMT can consider adding 1 step.
- Condition: MI SMT will find the best strategy to apply the new salary scale, ensuring the change will not burden MI's annual financial performance. For example, if a staff member does not reach a new salary, they can increase the percentage of the annual performance rating to those who reach a new salary scale.
- The new salary scale will attract highly qualified and experienced staff while keeping the current staff moving on according to their job level and step. As such, it is hoped that all staff will contribute to the organization's achievement and deliver quality work.

5.2 Revised Organization Structure:

- SMT will discuss, announce and put the staff in the positions of the structure.
- The expected duration of implementation of the new structure will start from January 2024 onward.

5.2 Revised Operation Manual, Parts:

- MI will rewrite and edit the language of the Operations Manual, which will be responded by the DFO and CMK Team

---

Annex I

Committee Members for the revision of MI Operations Manual in 2020 consist of:

- Mr. Suriyan Vichitlekarn – Executive Director
- Mr. Madhurjya Kumar Dutta – Director of Trade and Investment Facilitation Department
- Ms. Maria Theresa S. Medialdia – Director of Agricultural Development and Commercialization Department
- Mr. Rithy Buth - Director of Finance and Operations Department
- Mr. Sudam Pawar – Senior Consultant
- Ms. Phinyada Foytong - Finance Manager
- Ms. Jutamas Thongcharoen - Program Manager
- Mr. Mohammad Halimur Rahman – Monitoring, Evaluation and Learning Specialist
- Ms. Chonthicha Faypen - General Service Supervisor
- Ms. Vitchaya Panurak - Human Resource Officer

✓ Approved by MI Council on December 16, 2021
✓ Announced by Executive Order 007/2021 on March 1, 2021

Annex 2: Revised Staff Salary Scale

Mekong Institute

Annual MI New Salary Scale

From mid 2024 or 2025 (Proposed salary scale = 20% for M1, 50% for M2, 40% for M3-M4 , 30% for M5-M6 and 5% for M 7-M11)

USD

Annual Values USD - Base

Classification	Job Level	Position Titles		Initial Offer	Learning Zone Steps			Qualifying Zone Steps					Premium Zone Steps						
				Entry	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV
		Program	Corporate Services																
Directorship 0	M0	Executive Director			102,000	107,100	112,200	117,300	122,400	127,500	132,600	137,700	142,800	147,900	153,000	158,100	163,200	168,300	173,400
Directorship 1	M1				99,360	104,328	109,296	114,264	119,232	124,200	129,168	134,136	139,104	144,072	149,040	154,008	158,976	163,944	168,912
Professional 5	M2	Director of Program, Director of Project, MEL Director	CKM Director, Director of Finance and Operations	61,073	67,859	71,252	74,645	78,038	81,431	84,824	88,217	91,610	95,003	98,396	101,789	105,182	108,575	111,968	115,360
Professional 4	M3	Program Specialist, MEL Specialist, Project Team Leader	Finance Manager, HR Manager	42,223	46,915	49,261	51,606	53,952	56,298	58,644	60,989	63,335	65,681	68,027	70,372	72,718	75,064	77,410	79,755
Professional 3	M4	Program Manager	External Relations Manager	31,277	34,752	36,489	38,227	39,965	41,702	43,440	45,177	46,915	48,653	50,390	52,128	53,865	55,603	57,340	59,078
Professional 2	M5	Program Coordinator, Field Coordinator, M&E Coordinator	Supervisor, Communication Coordinator	22,340	24,823	26,064	27,305	28,546	29,787	31,028	32,270	33,511	34,752	35,993	37,234	38,475	39,716	40,957	42,199
Professional 1	M6	Program Officer, Project Officer	HR Officer, Communication Officer	17,185	19,094	20,049	21,004	21,959	22,913	23,868	24,823	25,777	26,732	27,687	28,642	29,596	30,551	31,506	32,460
General Support (GS5)	M7		Procure. Off, Project Finance Off, Cash& Bank Off, Ex. Assistant, General	12,437	13,819	14,510	15,201	15,892	16,583	17,274	17,965	18,656	19,347	20,037	20,728	21,419	22,110	22,801	23,492
GS4	M8	Field Assistant	Admin Assistant	9,567	10,630	11,161	11,693	12,224	12,756	13,287	13,819	14,350	14,882	15,413	15,945	16,476	17,008	17,539	18,071
GS3	M9	Program Assistant	Admin Receptionist	7,359	8,177	8,586	8,995	9,403	9,812	10,221	10,630	11,039	11,448	11,856	12,265	12,674	13,083	13,492	13,901
GS2	M10		Driver, Technician Senior Housekeeper	5,661	6,290	6,604	6,919	7,233	7,548	7,862	8,177	8,491	8,806	9,120	9,435	9,749	10,064	10,378	10,693
GS1	M11			4,355	4,838	5,080	5,322	5,564	5,806	6,048	6,290	6,532	6,774	7,016	7,258	7,500	7,741	7,983	8,225

Note:
- From entry to first step = 10% for probation period
- Between steps = salary adjustment is based from Step 1 (base salary) at increasing increments of 5% per grade.
- Declining rate of annual increase
- The salary steps have been expanded up to step 15 following the salary structure and formular of the approved current salary scale.
- Step 15 shall be the ceiling step and therefore no more steps to be expanded beyond the ceiling step.

Annual MI Salary Scale

Source: revise the staff salary scale on November 27, 2023

USD

Classification	Job Level	Current salary scale - Level 1	MI Team Analysis and consultant		Consultant Firm		UN Website		Propose to Council	
		Annual Salary	Annual Salary	% increase/decreased	Market Annual Salary	% increase/decreased	Annual Salary	% increase/decreased	Annual Salary	% increase/decreased
Directorship 0	M0	102,000	142,800	40%	104,460	2%	NA		102,000	0%
Directorship 1	M1	82,800	115,920	40%	104,460	26%	NA		99,360	20%
Professional 5	M2	45,239	63,335	40%	79,760	76%	92,962	105%	67,859	50%
Professional 4	M3	33,511	46,915	40%	60,269	80%	73,962	121%	46,915	40%
Professional 3	M4	24,823	34,752	40%	47,009	89%	58,837	137%	34,752	40%
Professional 2	M5	19,094	26,732	40%	28,090	47%	58,837	208%	24,823	30%
Professional 1	M6	14,688	20,563	40%	18,646	27%	47,220	221%	19,094	30%
General Support (GS5)	M7	13,161	18,425	40%	12,165	-8%	25,682	95%	13,819	5%
GS4	M8	10,124	14,173	40%	9,408	-7%	21,246	110%	10,630	5%
GS3	M9	7,788	10,903	40%	6,225	-20%	16,868	117%	8,177	5%
GS2	M10	5,990	8,387	40%		-100%	13,494	125%	6,290	5%
GS1	M11	4,608	6,451	40%		-100%	10,795	134%	4,838	5%

Annual MI Salary Scale

From 2014 (Proposed salary scale = 53% for M2-M6 and 60% for M 7-M11) - Reviewed January 2016 -

USD

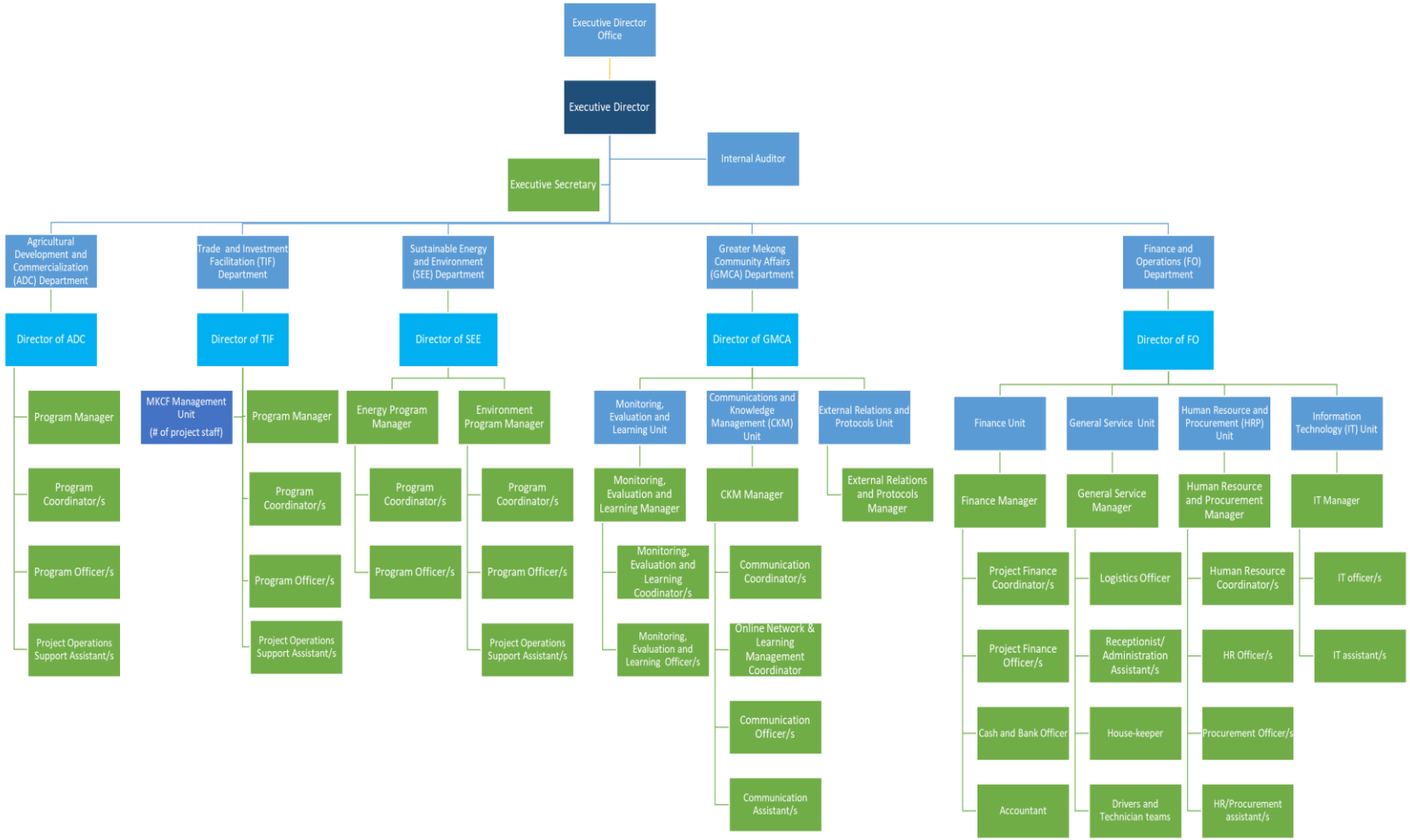
Annual Values USD - Base

Classification	Job Level	Position Titles			Initial Offer	Learning Zone Steps			Qualifying Zone Steps					Premium Zone Steps						
		Program	Corporate Services		Entry	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV
Directorship 0	M0	Executive Director				102,000.00	107,100.00	112,200.00	117,300.00	122,400.00	127,500.00	132,600.00	137,700.00	142,800.00	147,900.00	153,000.00	158,100.00	163,200.00	168,300.00	173,400.00
Directorship 1	M1					82,800.00	86,940.00	91,080.00	95,220.00	99,360.00	103,500.00	107,640.00	111,780.00	115,920.00	120,060.00	124,200.00	128,340.00	132,480.00	136,620.00	140,760.00
Professional 5	M2	Director of Program, Director of Project, MEL Director	CKM Director, Director of Finance and Operations		37,699.51	45,239.41	47,501.38	49,763.35	52,025.32	54,287.29	56,549.26	58,811.23	61,073.20	63,335.17	65,597.14	67,859.11	70,121.08	72,383.05	74,645.02	76,906.99
Professional 4	M3	Program Specialist, MEL Specialist, Project Team Leader	Finance Manager, HR Manager		27,925.56	33,510.67	35,186.21	36,861.74	38,537.27	40,212.81	41,888.34	43,563.87	45,239.41	46,914.94	48,590.47	50,266.01	51,941.54	53,617.08	55,292.61	56,968.14
Professional 3	M4	Program Manager	External Relations Manager		20,685.60	24,822.72	26,063.86	27,304.99	28,546.13	29,787.26	31,028.40	32,269.54	33,510.67	34,751.81	35,992.94	37,234.08	38,475.22	39,716.35	40,957.49	42,198.62
Professional 2	M5	Program Coordinator, Field Coordinator, M&E Coordinator	HR Coordinator, GS Supervisor, Communication Coordinator		15,912.00	19,094.40	20,049.12	21,003.84	21,958.56	22,913.28	23,868.00	24,822.72	25,777.44	26,732.16	27,686.88	28,641.60	29,596.32	30,551.04	31,505.76	32,460.48
Professional 1	M6	Program Officer, Project Officer	HR Officer, Communication Officer		12,240.00	14,688.00	15,422.40	16,156.80	16,891.20	17,625.60	18,360.00	19,094.40	19,828.80	20,563.20	21,297.60	22,032.00	22,766.40	23,500.80	24,235.20	24,969.60
General Support (GS5)	M7		Procur. Off, Project Finance Off, Cash& Bank Off, Ex. Assistant, General Service Off, GMS resource Off.		10,967.42	13,160.91	13,818.95	14,477.00	15,135.05	15,793.09	16,451.14	17,109.18	17,767.23	18,425.27	19,083.32	19,741.36	20,399.41	21,057.45	21,715.50	22,373.54
GS4	M8	Field Assistant	Admin Assistant		8,436.48	10,123.78	10,629.96	11,136.15	11,642.34	12,148.53	12,654.72	13,160.91	13,667.10	14,173.29	14,679.48	15,185.66	15,691.85	16,198.04	16,704.23	17,210.42
GS3	M9	Program Assistant	Admin Receptionist		6,489.60	7,787.52	8,176.90	8,566.27	8,955.65	9,345.02	9,734.40	10,123.78	10,513.15	10,902.53	11,291.90	11,681.28	12,070.66	12,460.03	12,849.41	13,238.78
GS2	M10		Driver, Technician Senior Housekeeper		4,992.00	5,990.40	6,289.92	6,589.44	6,888.96	7,188.48	7,488.00	7,787.52	8,087.04	8,386.56	8,686.08	8,985.60	9,285.12	9,584.64	9,884.16	10,183.68
GS1	M11				3,840.00	4,608.00	4,838.40	5,068.80	5,299.20	5,529.60	5,760.00	5,990.40	6,220.80	6,451.20	6,681.60	6,912.00	7,142.40	7,372.80	7,603.20	7,833.60

Note: From entry to first step = 15% salary adjustment for all levels and 20% for M 3 and M 2
Between steps = salary adjustment is based from Step 1 (base salary) at increasing increments of 5% per grade.
Declining rate of annual increase

The salary steps have been expanded up to step 15 following the salary structure and formular of the approved current salary scale.
Step 15 shall be the ceiling step and therefore no more steps to be expanded beyond the ceiling step.
The expansion of salary steps are the interim solution to the long-term employment of MI staff who have reached step 10.

Annex 3: Revised Organization Structure



Annex 3: Revised Operation Manual, Parts

Section	Current Policy	Proposed Revision	Page
Human Resources Unit			
PART ONE: MEKONG INSTITUTE PART ONE: MEKONG INSTITUTE ORGANIZATION ORGANIZATION (New part)	Mission	**Mission:** To contribute through human resource development and capacity building to the acceleration of sustainable economic and social development and poverty alleviation in the Greater Mekong Sub-region and promote regional cooperation and integration.	
	Purposes	**Purposes:** - To facilitate the promotion of state competence and efficient, effective and transparent governance and corporate administration in the Greater Mekong Sub-region (GMS) and to improve the welfare of our people - To design and deliver high-quality, relevant human resource development programmes for senior and mid-level officials, private sector and non-government representatives of the Greater Mekong Sub-region in the areas of sustainable development, poverty alleviation, integration and management reform - To implement a research programme, which contributes to the effectiveness of Institute courses - To promote effective regional cooperation amongst the governments and other organizations of the Greater Mekong Sub-region	
	Values	**Values** - Leadership: in teaching and research in planning, management and implementation of sustainable development and transition economics - Collaboration: with the governments of the Greater Mekong Sub-region, with public and private organizations and institutions with comparable goals - Accountability: for implementing the Institute's Mission and educational purpose and for ensuring effective management of its resources - Development: of participants and staff - Excellence: in teaching and research	

		- Freedom: from discrimination on the grounds of the difference in origin, race, language, sex, age, economic or social standing, religious belief or political view - Consultation and communication: internally and externally	
HRP-002 CODE OF CONDUCT	New	**2.4 Avoiding Conflicts of Interest** A conflict of interest is any activity that may damage MI's reputation or financial interests, or gives the appearance of impropriety or divided loyalty. Avoid any situation that creates a real or perceived conflict of interest. The following are common situations staff may encounter that could present a conflict of interest. • **Significant Personal Relationships:** Personal relationships in the workplace can present a real or perceived conflict of interest when one individual in the relationship makes or influences employment decisions regarding the other, including performance or compensation. Significant personal relationships include, but are not limited to, spouses, domestic partners, family members, dating or physical relationships, close friends, and business relationships outside of MI. MI business relationships include, but are not limited to, vendors, suppliers, contractors, temporary agency workers, or similar relationships. • **Conflicts of Interest and Outside Activities:** You may participate in outside activities, including secondary employment, businesses, inventions, and serving on boards, only if they do not present a conflict of interest and must comply with the following rules. Do not:	8

		➢ Use any time at work or any MI assets for your outside activity. This includes MI's workspace, phones, computers, Internet access, photocopiers, and any other MI assets or services. ➢ Use your position at MI to solicit resources or any other benefit for your outside activity, obtain favored treatment, or pressure others to assist you. ➢ Participate in an activity that could have an adverse effect on your ability to perform your duties at MI. ➢ Use confidential MI information. • **Outside Employment and Inventions:** Before participating in creating inventions or services that are in the same area as your work for MI, or that compete with or relate to MI's present or reasonably anticipated business, products, or services, you must have written permission from the Executive Director. Before taking any paid employment outside of MI, you should notify your supervisor. **When to Disclose:** 1) At Hire - New staff members must submit a Conflict of Interest Disclosure Statement. 2) Annually - Staff must submit a Conflict of Interest Disclosure Statement in January of each year, even if there are no changes from the prior year. 3) When a new conflict of interest arises - Staff must update their last submitted Conflict of Interest Disclosure Statement before or as soon as possible after the new conflict of interest arises, but in no case later than thirty (30) days after the interest arises. Please note that such an interest may arise due to new interests acquired by the staff member (such as the acquisition of new assets or income sources through purchase, marriage, or inheritance) or due to new responsibilities at MI (for example, participation in a research activity funded by an entity in which the staff member has a conflict	

		of interest). If possible, a new conflict of interest should be disclosed before the interest arises to minimize disruption of the activities of the staff member and MI.	
HRP-013: Education Allowance	The MI shall reimburse 75% of actual education fees (which included: tuition fee, books and library, language courses) for up to a maximum of two eligible child dependents, up to a maximum amount of the equivalent of USD 8,000 per child per academic year.	The MI shall reimburse 75% of actual education fees (which included: tuition fee, books and library, language courses) for up to a maximum of two eligible child dependents, **up to a maximum amount of the equivalent of USD 10,000 per child per calendar year.**	52
HRP-009: Leave	(1) Exceptional circumstances in which a staff may request compensatory time off are: shortage of staff; when requested to work on a public holiday or weekend facilitating a training or meeting; or being required to undertake official travel on a public holiday or weekend day on two or more holidays or weekend days per trip. Compensatory time off should be requested by the staff in advance, and considered and approved by the Department Director. However, if the staff member is paid facilitation or other fees for work during the non-working days, no compensatory days off may be claimed.	(1) Exceptional circumstances in which a staff may request compensatory time off are: shortage of staff; when requested to work on a public holiday or weekend facilitating a training or meeting; or being required to undertake official travel on a public holiday or weekend day on two or more holidays or weekend days per trip. Compensatory time off should be requested by the staff in advance, and considered and approved by the Department Director. However, if the staff member is paid facilitation or other fees for work during the non-working days, no compensatory days off may be claimed. **In the event that a staff member works during their travel days, the supervisor may evaluate the need to grant compensatory days in addition to the daily subsistence allowance.**	40
HRP-009: Leave	Compensatory leave shall be utilized within 2 months of its accrual; otherwise it will be forfeited. The Executive Director may grant an extension in exceptional circumstances.	Compensatory leave shall be utilized **within 3 months of its accrual**; otherwise it will be forfeited. The Executive Director may grant an extension in exceptional circumstances.	40
HRP-010: Relocation And Assignment Allowances	Provided that the total amount of freight does not exceed USD 2,000 each way. Eligible dependents include the legal spouse of the staff member and children below 18 years of age. The number of	Provided that the total amount of freight does not exceed USD 2,000 each way. Eligible dependents include the legal spouse of the staff member and children below 18 years of age. The number of eligible dependents is limited to a maximum of three, including the spouse.	

	eligible dependents is limited to a maximum of three, including the spouse. Shipment entitlement on return to home country at separation is paid provided that the staff member has served MI for at least one year.	**Shipment entitlement from the home country is expected to be completed within four months from the joining date**. **Upon separation, the shipment entitlement for the return to the home country is granted, contingent upon the staff member having served MI for at least one year. Staff members are required to complete the shipment within one month from termination date.**	
HRP-010: Relocation And Assignment Allowances	(3) The assignment allowance is USD 600.	(3) The assignment allowance is **USD 800**.	46
HRP-010: Relocation And Assignment Allowances	Shipment entitlement on return to the home country upon separation is provided, provided that the staff member has served MI for at least one year.	Shipment entitlement on return to the home country upon separation is provided, provided that the staff member has served MI for at least one year. **Taxes imposed on goods when transported across international borders are not reimbursable**.	45
HRP - 004 TERMS OF EMPLOYMENT	4.2.4 All staff members are normally offered a fixed-term one year contract with a probationary period of three months. During the probationary period, both the employee and the MI have the right to terminate the employment by giving a one-week written notice to the other party. 4.2.5 All fixed-term appointments carry no expectation of renewal and expire automatically and without notice on the expiration date specified in the Employment Contract. Contracts may be renewed based on budget, organizational requirements, and staff performance. 4.2.6 The first and the second contract renewals will be based on yearly basis. From the third	4.2.4 **All staff members, with the exception of those employed at job level M2,** are normally offered a fixed-term one year contract with a probationary period of three months. During the probationary period, both the employee and the MI have the right to terminate the employment by giving a one-week written notice to the other party. 4.2.5 All fixed-term appointments carry no expectation of renewal and expire automatically and without notice on the expiration date specified in the Employment Contract. Contracts may be renewed based on budget, organizational requirements, and staff performance. 4.2.6 The first and the second contract renewals will be based on yearly basis. From the third renewal, term of contract can be considered as 3- years basis, depends on availability of fund. 4.2.7 **Staff members employed at job level M2 are offered a fixed-term three-year contract, accompanied by a probationary period of three months. During the probationary period, both the employee**	18

	renewal, term of contract can be considered as 3-years basis, depends on availability of fund.	**and MI have the right to terminate the employment by providing one week's written notice to the other party. The contractual commitment may extend for up to two terms, reaching a maximum period of six years. After reaching the maximum terms, the contract may be extended to a one-year term with annual renewals for a maximum of two years, subject to budget considerations, organizational requirements, and staff performance.**	
HRP-003 RECRUITMENT AND SELECTION	New	The job advertisement should include the annual salary scale or range, as well as a concise benefits package, to establish clear expectations for both the employer and the prospective employee.	15
Flexible Hours	New	Official working hours are from 08:30 to 17:00, Monday through Friday, except for holidays. The definition of official working hours aligns with MI's operating hours, during which the organization is in operation and available for external parties. Total hours are 8.50, including lunch for one hour. -Staff has the flexibility to arrive between 08:30 and 09:00 without the necessity of advance notice and/or seeking permission from their supervisor. -If a staff member arrives after 10:00, it will be considered their half-day morning leave.	
Remote Work Policy (New Policy)	New	1. Rationale: 1.1 To respond to evolving work trends that emphasize the importance of providing flexibility to our workforce. 1.2 To support the well-being of our staff by offering a balanced approach to work, recognizing the need for flexibility in today's dynamic work environment. 1.3 To ensure that the operational effectiveness and productivity of our organization are maintained at high standards. 2. Policy and General Provisions:	

		2.1 Eligibility: This policy applies to all staff members, subject to the discretion of departmental management. Not all roles may be suitable for remote work, and decisions will be based on operational needs and individual performance. 2.2 Remote Work Arrangements: Staff may be permitted to work remotely based on their eligibility and approval from their respective supervisors. Remote work arrangements may be temporary or long-term, depending on business needs and individual circumstances. 2.3 Request and Approval Process: Staff must formally request remote work, specifying the duration, proposed working hours, and an outline of tasks to be accomplished. Supervisors will review requests, considering operational requirements, team collaboration, and individual performance. 2.4 Equipment and Connectivity: Staff are responsible for ensuring they have the necessary equipment and a secure internet connection for remote work. The organization may provide resources or reimburse expenses, subject to prior approval. 2.5 Security and Confidentiality: Staff must adhere to security and confidentiality measures to protect organizational information during remote work. Compliance with data protection protocols is mandatory. 3. Guidelines:	

		3.1 Working Hours: Staff must adhere to their regular working hours as specified in their employment agreement unless otherwise agreed upon with their supervisor. 3.2 Accessibility: During remote work, staff must be accessible during working hours through email, phone, or other agreed-upon communication channels. 3.3 Productivity and Goals: Staff are expected to maintain productivity levels and achieve established work goals during remote work. 3.4 Meetings and Communication: Remote staff are required to participate in virtual meetings and maintain regular communication with team members and supervisors.	
HRP-009 LEAVE	EXECUTIVE ORDER: EO 2023-05	Home Leave is designed to allow regular international and GMS staff members, along with accompanying dependents, periodic visits to their home country to restore, maintain, and strengthen cultural and family ties. 1)The staff member must complete one year of service with Mekong Institute. Afterward, they must continue employment with MI for at least six (6) months upon returning from home leave. 2)Home leave is an annual entitlement that cannot carry forward to the following year. However, carryover is permitted due to the effects of official assignments and is subject to approval by the supervisor and the Executive Director in advance. In general, it is expected that staff will be able to take home leave entitlement within the annual leave year. Therefore, the above provision will apply to a limited number of staff and on a case-by-case basis.	40

		3)All receipts, invoices, and supporting documents must be submitted to HR and Finance units for clearance one month after returning to the office. 4)MI will not cover any additional costs incurred due to personal requests. 5)The leave period shall be applied to the annual leave and/or leave without pay. A maximum of two travel days shall be considered as work days.	
HRP - 024 INTERNSHIP, VOLUNTEERS and VISITING SCHOLARS	New	24.3.3 Terms and Conditions Conditions for Trainee • The trainee shall receive a stipend of 5 USD per day. s/he will receive the stipend only on working days. Trainees who receive support from external entities, including but not limited to government sponsors and grants that incorporate a Cost of Education allowance or similar benefits, are ineligible for the stipend.	95
General Service Unit			
ADM-008: Travel	**"Official travel by private vehicle must be authorized before departure. Concerned Staff members have to obtain prior authorization from the Executive Director. The rate of reimbursement is THB 5 (five baht) per kilometer which includes gas, oil, wear and tear. Charges for parking fees and tolls paid by the traveler can be reimbursed upon presentation of actual receipts. MI will not be responsible for paying other costs such as vehicle insurance, border crossing costs etc.**	**" Official travel by private vehicle must be authorized before departure. Concerned Staff members have to obtain prior authorization from the Executive Director. The rate of reimbursement is** THB 7 (seven baht) **per kilometer which includes gas, oil, wear and tear. Charges for parking fees and tolls paid by the traveler can be reimbursed upon presentation of actual receipts. MI will not be responsible for paying other costs such as vehicle insurance, border crossing costs etc. The standard distance will be used for the calculation."**	130

	The standard distance will be used for the calculation."		
ADM-008: Travel	"a. Travel allowance within Thailand can be requested in advance and will be paid at THB 500 per day for meals and incidentals (Refer to travel advance)."	"a. Travel allowance within Thailand can be requested in advance and will be paid at **THB 800 per day** for meals and incidentals (Refer to travel advance)."	133
ADM-008: Travel	**"• If the travel period is 4 hours and less, this is considered a half day travel and therefore, the travel allowance will be THB 250** **• If the travel period covers more than 4 hours, the full amount of Baht 500 will be issued** **c. MI will pay for the actual hotel accommodation cost up to USD 100 per night. If the cost is more than USD 100, a request for an ad-hoc rate should be made in advance."**	**"• If the travel period is 4 hours and less, this is considered a half day travel and therefore, the travel allowance will be** THB 400 **• If the travel period covers more than 4 hours, the full amount of** Baht 800 **will be issued** **c. MI will pay for the actual hotel accommodation cost up to** USD 120 **per night. If the cost is more than USD 100, a request for an ad-hoc rate should be made in advance."**	134
ADM-008: Travel	" Travel outside Thailand by MI Secretariat staff, or travel outside of country of assignment for FO staff a. Travel allowance within Asia for meals and incidentals is USD 50 per day and USD 80 per day for travel outside of Asia. b. Travel begins from starting point to destination; Therefore, the travel allowance is also counted from the starting point to destination.	" Travel outside Thailand a. Travel allowance within Asia for meals and incidentals is **USD 60** per day and **USD 90** per day for travel outside of Asia. b. Travel begins from starting point to destination; Therefore, the travel allowance is also counted from the starting point to destination. c. If accommodation is not provided by the organizer, MI will pay for the actual hotel accommodation cost up to **USD 120** per night. If	134

	c. If accommodation is not provided by the organizer, MI will pay for the actual hotel accommodation cost up to USD 100 per night. If the cost is more than USD 100, a request for an ad-hoc rate should be made in advance to be approved by the Executive Director. **Travel by FO staff within their country of assignment:** **a. Travel allowance is payable for meals and incidentals during travel within the province to the field after 70 Kilometers from their duty station.** **- The travel allowance is the local currency equivalent of THB 500 per day.** **- Travel allowance is paid based on number of night(s) that staff has to stay away from home for working purpose.** **- The travel allowance is not eligible when staff travelled forward and back within a day.** **b. Travel allowance payable for meals and incidentals during travel to another province within their country of assignment is the local currency equivalent of THB 500 per day.** **c. MI will pay for the actual hotel accommodation cost up to the local currency equivalent of USD 80 per night. If the cost is more than USD 80, a request for an ad-hoc rate should be made in advance."**	the cost is more than **USD 120**, a request for an ad-hoc rate should be made in advance to be approved by the Executive Director."	
Procurement Unit			

HRP-009 Procurement Rationale	9.1.1 To acquire goods and services for MI in such a manner as to maximize the value to MI with respect to price, quality, service availability and operational performance. 9.1.2 To establish a systematic purchasing policy and procedures for all MI staff to follow in order to obtain the best value for money and in accordance with the well-establish procedures which are applied by most international organizations. 9.1.3 To improve efficiency and effectiveness of the procurement process and to promote consistent application of best procurement practices. 9.1.4 To ensure the basic principles of public procurement including transparency, integrity and accountability, competition, value for money, and economy and efficiency apply to all MI's purchasing activities.	9.12 Cost Efficiency: The Procurement unit team identifies cost-effective suppliers, negotiate favorable terms and prices, leveraging economies of scale to reduce overall costs. The unit is involved in proper procurement management, which helps in optimizing the allocation of resources and budget utilization, ensuring that funds are used effectively. 9.13 Supplier Management: The procurement unit at MI assesses and selects suppliers based on criteria such as quality, reliability, reputation, and financial stability. This leads to establishing and maintaining relationships with suppliers to facilitate smooth transactions, resolve issues, and ensure a steady supply of goods and services to MI. 9.14 Risk Mitigation: At MI the Procurement unit works to diversify the supplier base and create contingency plans to mitigate disruptions in the supply chain. The unit also ensure that MI complies with Thai laws, regulations, and ethical standards related to procurement, reducing legal and reputational risks. 9.15 Quality Assurance: The unit collaborates with programs, IT and finance units as the case may be to define clear products or service specifications, ensuring that purchased items or services meet MI organizational needs and quality standards. In addition, the unit oversees quality control processes to ensure that goods and services conform to agreed-upon standards. 9.16 Process Efficiency:	136

		MI Procurement unit designs and streamlines processes to implement efficient procurement procedures that minimize delays and paperwork, facilitating quicker access to needed resources. The unit also utilizes procurement software and technology to automate routine tasks, improve data analysis, and enhance decision-making. 9.17 Accountability and Transparency: The unit maintains detailed records of procurement activities, promoting transparency and accountability. This facilitates expeditious internal and external audits that enhance compliance and provide timely reports to management on procurement performance. 9.18 Strategic Alignment: MI procurement unit aligns its strategies with the overall goals and objectives of the organization, contributing to its success. The unit identifies opportunities for strategic sourcing, which involves selecting suppliers based on long-term partnerships and value-added services rather than just cost to Mekong Institute.	
9.3.4 Authorization Limit Signing authority for Purchase request	(3) The actual purchasing function rests with the Procurement Unit. Other staff members (except finance staff) can perform actual purchases only with prior approval of the Purchase Requisition (PR) and if the value of a one-time purchase is not more than USD 100.	The actual purchasing function rests with the Procurement Unit. Other staff members (except finance staff) can perform actual purchase only with prior approval of the Purchase Requisition (PR) and if the value of a one-time purchase is not more than USD 500	
9.3.5 Procurement Thresholds	Up to USD 100 Single source quotation PR	Up to USD 500 Single source quotation PR	

	Receipt Unit Head PO / Contract- N/A	Receipt Director PO / Contract- N/A	
	From USD 100 to USD 500 Informal competition PR 3 informal quotes Invoice/Receipt / PO	From USD 500 to USD 1,000	
	From USD 500 to USD 1000 Formal Competition • PR • Invite to quote • 3 formal quotes • Invoice/Receipt • PO/Contract	From USD 1,000 to USD 5,000	
9.3.7 Procurement Methods	(1) Low Value Low value procurements are those normally procured in cash or equivalent mode. Low value procurement may be used in the following circumstance: i.The estimated cost of goods, works or services for a one time purchase is less than or equal to the prescribed maximum value as set out in the Threshold (up to USD 100);	(1) Low Value Low value procurements are those normally procured in cash or equivalent mode. Low value procurement may be used in the following circumstance: i.The estimated cost of goods, works or services for a one time purchase is less than or equal to the prescribed maximum value as set out in the Threshold (up to USD 500);	148
	Request for Quotations I Informal Request for Quotations	Request for Quotations	

	When goods or services are estimated to cost between USD100 & USD 500	An informal Request for Quotations is unnecessary when goods or services are estimated under USD 500. We need formal quotations when goods or services are estimated to cost over 500 to 1000 USD.	
	(3) Open Tender When the costs of required goods or services are estimated to exceed USD 25,000, an open tender will be considered as the most appropriate method of MI procurement. The invitation to bid will indicate brief particulars of the product, quantity, eligibility of the companies/enterprises to participate in MI bidding, destination where the goods or services are to be delivered, the name and address of the office where bid documents can be obtained, closing date for receipt of tenders and specified place for submission of tenders. The bid documents containing detailed specifications, bid conditions and instructions to bidders shall be also advertised in the leading newspapers in the GMS region or business opportunity forum.	Open Tender and Bid selection process: Rationale: The open tender and bid selection processes are essential components of procurement and contract management in Mekong Institute. These processes managed by the Procurement unit are designed to ensure fairness, transparency, and competitiveness in the procurement of goods, services, and projects. In MI, the Procurement unit undertake and leads these processes: 1 Open Tender Process: - Identification of Need: The process begins with the Unit/Dept begin for goods, services, or project work. This need is triggered by various factors from the Unit/Dept, such as project requirements, maintenance needs, or supply demands. The Unit/Dept must have available funds set aside in the budget for these purposes. - Preparation of Tender Documents: Detailed tender documents are prepared by the Procurement unit that outline the project requirement specifications, terms and conditions, evaluation criteria, and submission instructions. These documents must be clear, comprehensive, and fair to all potential bidders. - Advertisement: The Procurement unit publicly advertised the tender to attract a wide range of potential bidders. This includes publishing notices in newspapers, on websites, or through specialized procurement platforms.	

		- Bid Submission: Interested bidders submit their sealed bids or proposals by the specified deadline, set by the Procurement unit. The bids include technical proposals, price quotes, and any required supporting documents. - Bid Opening: The Procurement unit sets a specified date and time, to conduct a bid opening ceremony in which the submitted bids are opened and recorded. This process ensures transparency and accountability that are enshrined in the procurement processes in MI. - Bid Evaluation: MI in consultation with the Procurement unit selects a team of experts or evaluators to assess the bids based on the pre-defined evaluation criteria, which may include technical qualifications, experience, financial stability, and price. The goal of the Expert committee is to determine the most qualified and cost-effective bidder. - Selection of Successful Bidder: The Procurement unit selects the successful bidder, after the evaluation process who is awarded the contract. The Procurement unit's decision is based on a combination of technical and financial factors. - Contract Negotiation: The PU commences with contract negotiations the successful bidder to finalize the terms and conditions of the contract. This includes discussing any necessary modifications and clarifications. - Contract Award: The contract is awarded to the selected bidder, and all unsuccessful bidders are notified of the outcome accordingly by the PU. The contract is signed by Director of Finance & Ops or the Executive Director depending on the authorization thresholds. 2 Bid Selection Process:	

		Rationale: At MI the bid selection process forms a crucial part of the open tender process and involves the evaluation and comparison of bids submitted by potential suppliers or contractors to the Procurement unit. These processes aim to ensure transparency, competition, and fairness while acquiring goods and services through a structured and regulated approach The Procurement unit takes these key considerations taken into account by and the bid selection committee set up for the purposes: - Evaluation Criteria: The PU establishes clear and predefined evaluation criteria, which include technical competence, experience, quality of goods or services, price, and compliance with tender requirements. - Bid Evaluation Committee: MI appoints a committee or team of experts who ensures objectivity and impartiality in the selection process to review and evaluate the bids. - Scoring and Ranking: The Committee ensures each bid is evaluated against the established criteria, and scores are assigned and ranked based on their scores to identify the most suitable bidder. - Selection Decision & Notification: The selection decision made by the Committee is based on a combination of factors, with the goal of selecting the bid that offers the best overall value to MI as an organization. All bidders are notified of the outcome once the selection is made.	

		- Contract Award: After the selection process is completed, the contract is awarded to the successful bidder, and negotiations may take place to finalize the contract terms.	
	New	9.3.8 Prevention of Fraud and Corruption Preventing fraud and corruption in MI requires a proactive and ongoing commitment to ethical practices, transparency, and accountability. Therefore, in MI a culture of integrity is enhanced to reduce the risk of fraud and corruption and uphold the mission to serve the public good. Preventing fraud and corruption in procurement processes at MI is crucial for maintaining the integrity and trustworthiness of a MI. MI has established ongoing vigilance, a commitment to transparency, and a culture of ethics and integrity throughout the organization. By implementing these measures, MI minimizes the risk of fraud and corruption in its procurement processes and ensures that donor funds are used effectively and responsibly.	151
	New Procurement Plan	All departments shall prepare and submit quarter procurement plan to procurement unit in January, April, July and October. The procurement will consolidate and submit the quarter procurement plan to DfoO and ED for reference and advice. The procurement will start the process in accordance with the request to be effective and on time.	
Communications and Knowledge Management Unit			
ADM-007 PUBLIC RELATIONS and PUBLICATION	7.1.1 To enhance the public perception corporate image of MI and the member countries' efforts to promote capacity building for regional cooperation and integration.	7.1.1 To enhance MI's efforts in implementing capacity development, dialogue and advocacy for regional cooperation and integration 7.1.2 To set up policies and procedures related to communication for consistent MI branding and smooth coordination	124

	7.1.2 To setup policies and procedures related to communication in order to create a forum in which for reliable and accurate information to can be made available and issues can be raised for discussion. 7.1.3 To establish policy and procedures related to publication in order to ensure that these publications are consistent with the purpose, produced economically, written according to international standards, and appropriate for the intended audience.	7.1.3 To establish policy and procedures related to publication to ensure that these publications are consistent with MI branding, purpose, produced economically, written according to international standards, and appropriate for the intended audience.	
ADM-007 PUBLIC RELATIONS and PUBLICATION	7.3.6 Learning Resource Center (1) A MI staff member, in coordination with other unit heads, shall be assigned to take responsibility for the selection of materials available at the center. (2) Only registered users are allowed to take out materials and resources from the center through a sign out procedure for a maximum loan period of 2 weeks. (3) At least one computer set with internet access shall be available to users on a first-come-first-served basis. (4) A photocopy machine shall be available to users and compliance to copyright laws shall be the responsibility of the users. MI shall strongly advise users of copyright laws and restrictions. (5) Users shall behave with respect and courtesy in consideration of other users and shall comply with center rules and regulations: a. Smoking, eating and drinking are not permitted at the center	Suggest to remove this section as MI no longer has a Learning Resource Center. Therefore, the texts are no longer applicable.	190

	b. Animals are not permitted at the center c. Silence must be observed in the center d. Equipment and furniture shall not be taken out of the center e. Users who fail to comply with center rules and regulations shall be asked to leave and/or barred from future entry and use of the center services.		
ADM-007 PUBLIC RELATIONS and PUBLICATION	7.4 Forms Used and References 7.4.1 MI annual reports, newsletters, minutes as samples 7.4.2MI Website 7.4.3 Learning Resource Center 7.4.4LRC Registration form	7.4 Forms Used and References 7.4.1 MI annual reports, newsletters, minutes as samples 7.4.2 MI Website ~~7.4.3 Learning Resource Center~~ ~~7.4.4 LRC Registration form~~ Suggest to delete 7.4.3 and 7.4.4 as they are no longer applicable.	193
Finance Unit			
FIN-001: General Financial Management	**(14) In addition to the above, the following reports must be produced at the end of each year: (i) Fund status reports for all closed project during the year and (ii) Fund status reports for all active projects (iii) cash and bank reconciliation (iv) aging report (v) financial statement and (vi) cash flow report. These records must be kept for annual audit and retained in according with retentions schedule**	**(14) In addition to the above, the following reports must be produced at the end of each month and year:** **At the end of month's financial report** **- Cash and bank reconciliation** **- Aging report** **- Statement of Financial Position** **- Statement of Comprehensive Revenue and Expense, including all valid projects such as** **Project Code, Project Title, Project Type, Donor's Name, Department's Name, Annual Budget/Revised Budget, Year-to-Date Budget, Year-to-Date Expense, % of Achievement, Variance and Remaining.**	

		-Program Departments Financial Report **- Donors' financial reports are based on the timeframe required.** **The finance will send the quarterly project financial report to program departments for reviewing and giving feedback.** **At the end-of-period financial report, the Finance Unit will need to prepare the following reports** **- Cash and bank reconciliation** **- Fund status reports for all closed projects and for all active projects during the year** **- Aging report** **- Statement of Financial Position** **- Financial statement** **- Cash flow report** **- Reserve Fund Report** **- Program Departments Financial Report** **These records must be kept for annual audit and retained according to the retention schedule**	
	(15) New (Set up the reserve fund for activities from Operations and Projects, which are supported by donors)	After closing the annual financial report, MI will divide the reserve into two parts: 1. Keep for future reserve and 2. Set up the reserve fund project to support the activities which are not sponsored. Director of Finance and Operations, supported by Finance Manager, will analyze and propose the reserve fund for future reserve and supported activities for Senior Management to consider and approve each year after the year-end with the confirmation of the result of MI's financial report by an external auditor	

FIN-002: Banking and Cash Management	**2.3.7 Currency Exchanges** **To minimize the exchange gain/loss from the exchange rate and show the real exchange rate when converting from US Dollars to Thai Baht, MI proposes:** **1. MI maintains its own currency exchange rates on a monthly basis. The rates are derived from the UN system of exchange rates.** **2. MI will apply the current month's exchange rates when the conversion is actually taken place unless there is a requirement from the funding agency. Source of monthly exchange rate will be taken and generated UN Operational Exchange rate in the first day of each month.**	**1. MI maintains its own currency exchange rates on a monthly basis. The rates are derived from the Bangkok Bank system in Khon Kean of exchange rates, MI shall obtain two times: day 1 and day 15 of the month,** **2. MI will apply the current month's exchange rates when the conversion is actually taken place unless there is a requirement from the funding agency. Source of monthly exchange rate will be taken and generated by the Bangkok Bank Exchange rate on day 1 and day 15 of the month.** **The reference bank may be subject to change upon approval from the Director of Finance and Operation and if the date mentioned is weekend or holiday, the rate of the day before will be applied**	
	New: Anti-Fraud/Corruption and Whistle-Blowing Policies	Anti-Fraud/Corruption and Whistle-Blowing Policies See the details in **"Note 1"**	
IT Unit: INFORMATION TECHNOLOGY SECURITY POLICY			
Please kindly see the INFORMATION TECHNOLOGY SECURITY POLICY in **"Note 2"**			

Note 1: Anti-Fraud/Corruption and Whistle-Blowing Policies

Anti-Fraud/Corruption and Whistle-Blowing Policies

1. Rationale

MI is committed to implementing its activities with a high level of responsibility, ethical standards, and integrity in collaboration with development partners, government agencies, and other supporting entities, whether through financial or in-kind contributions. To uphold these values, MI has developed and enforces the Anti-Fraud/Corruption and Whistle-Blowing Policy.

2. Anti-Fraud/Corruption

2.1 Purpose and Objectives

The anti-fraud/corruption policies at MI aim to promote accountability, transparency, and integrity within the organization. They play a pivotal role in ensuring that MI operates in an open and trustworthy manner, especially when working with funds provided by development partners and other agencies.

2.2 Enforcement

MI's senior management is responsible for enforcing the anti-fraud/corruption policy, recognizing the grave consequences fraud/corruption can have on the organization's effectiveness in achieving its vision, mission, and goals.

2.3 Definition of Fraud/Corruption

MI employees must be knowledgeable about what constitutes fraud/corruption and their role in preventing and detecting it within the workplace. Reference should be made to the Thai Anti-Corruption Law, approved by the Thai National Assembly, to avoid ambiguity in determining corrupt practices.

2.4 Focus Areas

MI places a strong emphasis on potential high-risk areas, including but not limited to:

Financial Records and Financial Management Guidelines, Systems, and Procedures
Information Technology and Communication Systems (ITC)
Procurement and Supply Chain
Human Resources and other relevant areas
Research and Reporting
MI Properties

- Financial Management and Controls
- Procurement and Supply Chain
- Human Resources
- Information Technology and Data Security
- Research and Reporting
- Donor Relations

- Whistleblower Protection
- Internal and External Audits
- External Collaboration
- Documentation and Record Keeping
- MI Properties

3. Whistle-Blowing

3.1 Reporting Wrongful Acts

Whistle-blowing occurs when an MI employee or service recipient has reasonable grounds to suspect wrongful acts within the organization. These acts can include any on-the-job activities that violate national laws, local ordinances, or organizational policies. Whistle-blowers are encouraged to report such acts to the Senior Management Team and Department Directors.

3.2 Protection for Whistle-Blowers

MI actively encourages employees to report wrongful acts in good faith. Those who report are referred to as 'whistleblowers.' Any attempt by a third party, including the accused, to obstruct a whistle-blower's reporting should result in disciplinary action, including possible dismissal.

3.3 Whistleblower Protection

MI is committed to protecting whistle-blowers from retaliation. Any retaliation against a whistle-blower will be promptly investigated by the anti-corruption committee designated by the MI Senior Management Team. Disciplinary action, up to and including dismissal, may be taken against employees found guilty of retaliation.

4. Anti-Terrorism

4.1 Compliance with Anti-Terrorism Laws

MI does not provide support of any kind to individuals or entities known or suspected to advocate terrorism or engage in terrorist activities. MI complies with all relevant laws and regulations addressing terrorism and terrorist activity.

4.2 Definition of Terrorist Activity

For the purpose of this policy, "terrorist activity" refers to any violent act intended to:

a) Intimidate or coerce a civilian population
b) Influence government policies through intimidation or coercion
c) Affect government conduct through mass destruction, assassination, kidnapping, or hostage-taking

5. Prevention Measures for Anti-Fraud/Corruption

5.1 Code of Conduct

MI shall adhere to and implement the Code of Conduct as outlined in the HR Section.

5.2 MI Operations Manual

MI strongly promotes and implements the MI Operations Manual.

5.3 Preventing Misuse of Procedures

MI is committed to preventing the misuse of its procedures and guidelines.

5.4 Promoting Accountability and Transparency

MI aims to foster accountability, transparency, honesty, integrity, and fairness among its staff and all parties involved in its transactions.

6. Roles and Responsibilities for Anti-Fraud/Corruption

All MI personnel, including the Senior Management Team, Directors of Departments, Managers, staff, and concerned parties, share the responsibility of ensuring that MI remains free from acts of fraud and corruption.

6.1 Senior Management Team (SMT)

- Develop and maintain an effective internal control system to prevent fraud and corruption.
- Handle all reports related to fraud and corruption.
- Establish a financial review committee to assess MI's internal controls periodically.
- Provide orientation on the fraud and corruption policy to all staff.
- Take appropriate actions in response to fraud and corruption cases.

6.2 Executive Director, Directors of Programs, Director of Finance and Operations, Finance Manager, and HR Manager

- Identify potential daily risks, including risks related to systems, procedures, and personnel.
- Implement and maintain internal controls to detect fraud and corruption.
- Continuously monitor and control risks.

Process for Handling Corruption and Fraud Cases:

1. Detection:

Corruption or fraud is detected through various channels, including internal audits, employee reports (whistleblowing), external tips, or routine financial and operational reviews.

2. Reporting:

Anyone who suspects corruption or fraud should report it promptly to their immediate supervisor, department head, or use the designated whistleblowing mechanism.

3. Initial Assessment:

The designated authority (e.g., Department Head or Senior Management Team) responsible for receiving reports initiates an initial assessment to determine the validity and severity of the allegations.

4. Notification:

If the initial assessment suggests a credible case of corruption or fraud, the matter is immediately reported to the Anti-Corruption Committee (ACC).

5. Anti-Corruption Committee (ACC):

The ACC should be an independent body within the organization responsible for handling corruption and fraud cases. It is typically composed of senior members from different departments to ensure objectivity and transparency. Recommended members of the ACC may include:

- A senior executive or member of the Senior Management Team (SMT) who serves as the Chairperson.
- The Director of Finance and Operations (DFO).
- The Head of Human Resources (HR).
- An External Expert (e.g., a legal advisor or an auditor).

The ACC should convene to review the case and make decisions regarding the investigation and corrective actions.

6. Investigation:

The ACC appoints an investigative team, which may include internal or external investigators with expertise in fraud and corruption investigations. The investigators conduct a thorough, impartial, and confidential investigation.

7. Findings and Recommendations:

The investigative team submits its findings and recommendations to the ACC, detailing the extent of corruption or fraud, the responsible parties, and proposed corrective actions.

8. Decision and Action:

The ACC reviews the findings and recommendations and decides on the appropriate actions to be taken. These actions may include:

- Disciplinary actions against the individuals involved.
- Legal action if applicable.
- Revisions to organizational policies and procedures to prevent future occurrences.
- Recovery of misappropriated funds or assets.
- Reporting to relevant authorities if necessary.

The ACC ensures that the actions taken are consistent with local laws and regulations.

9. Reporting and Communication:

- The ACC communicates the outcomes and actions taken to relevant stakeholders, including donors, government agencies, and employees (while respecting confidentiality and privacy laws).
- The organization maintains transparency to build trust with stakeholders.

10. Prevention and Monitoring:

The ACC monitors and evaluates the effectiveness of the corrective actions taken to prevent future occurrences of corruption and fraud.
Periodic reviews and audits are conducted to ensure ongoing compliance with anti-corruption policies.

11. Whistleblower Protection:

Throughout the process, the organization must protect whistleblowers from retaliation and ensure their anonymity, as mentioned in the Whistle-Blowing policy.

12. Continuous Improvement:

The organization continuously reviews and enhances its anti-corruption and fraud prevention measures based on lessons learned from each case and external developments.

Note 2: INFORMATION TECHNOLOGY SECURITY POLICY

Mekong Institute
Information Technology Services

INFORMATION TECHNOLOGY SECURITY POLICY

TABLE OF CONTENTS

1. Rationale

Information is a vital asset of Mekong Institute (MI), as is the information technology (IT) infrastructure that enables its collection, storage, processing and delivery of reports to our stake holders, donors and government institutions. The confidentiality and integrity of the information and availability of the IT infrastructure are crucial for ensuring the continued daily operations of MI.

This policy identifies the rules for all individuals accessing, using, maintaining, administrating or managing MI's information and IT infrastructure. Its objective is the preservation of confidentiality, integrity, and availability of the electronic resources used by the MI staff, partners, volunteers and occasional visitors. It endeavors to guide the establishment within MI of generally accepted information security practices and procedures as far as is reasonable and appropriate.

The purpose of the policy is to provide a clear statement to all users, administrators and managers of MI's IT facilities and services regarding their responsibilities, including what constitutes acceptable and unacceptable use; to manage the provision and modification of access to online services; and to express the commitment of MI to providing and maintaining secure, effective and reliable IT infrastructure to support MI's operations.

2. Scope

This policy applies to everybody who has authorized access to MI's network and systems.

The resources included in the scope of this security policy are electronic information, data, the computing hardware and software systems that access and manipulate information, and the network systems that transport the information and data. The resources may reside in many different settings and environments and may be used for operations, projects or administrative purposes.

3. Consequences of non-compliance

Non-compliance with this policy could lead to unavailability of resources, unauthorized access to information, corruption and loss of data, contravention of legislation, etc, and result in a substantial reduction in productivity, financial losses, fines or reputational damage to Mekong Institute.

Failing to comply or failing to report non-compliance with this policy or its supporting documents will be deemed as misconduct and line managers may initiate appropriate investigation and disciplinary action.

Note that users may be held personally responsible for any security breaches that occur because of their deliberate actions, inactions, or negligence.

4. Policy statement

IT unit is committed to the effective management of the security of all IT systems (data, equipment, and processes) and electronic information under its control. The implementation, maintenance and improvement of appropriate controls and security measures will be based on the identification, assessment and monitoring of security risks, with the objective of managing such risks and their impact on MI. However, this is not enough, and every person that uses, provides, or administrates information resources, has a responsibility to maintain and safeguard these assets.

Each authorized user in MI community is obligated to protect, to the best of their ability, the security (confidentiality, integrity and availability) of the IT infrastructure and MI institutional information collected, created, accessed or stored by them on personal computers or any other electronic devices under their jurisdiction/ownership. To this end they need to:

- keep informed on MI security policy and directives.
- protect MI information resources in any environment, shared or stand-alone, within the MI network or in the cloud; and
- use MI shared resources with consideration for others.

The policy is supported by several policies, standards, procedures and guidelines. Compliance with this policy requires compliance with all of these other supporting documents.

5. Clarification of security elements

The following aspects relating to security are included in the policy:

- security awareness
- physical and logical access management, including remote access and passwords.
- email and Internet usage
- malware protection and prevention
- service continuity and backups
- network and server security
- asset management, including handling of removable media and portable hardware.
- change management.
- system acquisition, development, and maintenance
- privacy and confidentiality
- compliance with law and policy
- management and reporting of security incidents
- management of security risks

5.1 Security awareness

Staff who have any form of oversight over employees, volunteers, contractors, vendors, guests and other users, must ensure that such persons are aware of requirements and expectations for information and technology security in accordance with this policy and its supporting documents.

The IT unit is responsible to provide:

- regular updates on this policy and its requirements to users.
- regular communication on security issues to sensitize users to current security risks; and
- training and advice to enable users to work responsibly with IT assets and resources and protect the security of MI and their own private information.

Users must take note that their adherence to security policy, responsible behavior and security awareness play a significant role in reducing MI's risk exposure.

5.2 Logical access and password control

ITS will manage logical access controls across its networks, IT systems and services to provide authorized, auditable and appropriate user access to Mekong Institute IT infrastructure, systems and services, as well as MI-owned end-user devices.

In order to achieve this, MI must:

- implement formal user access management processes to assign and revoke access rights for all user types to all systems and services.
- grant access rights based on an individual's role in MI and limit such access to resources required for performing their responsibilities;
- regularly audit privileged access rights;
- implement authorized access through the use of unique user identification codes and confidential passwords.

Users must:

- select passwords that comply with minimum requirements;
- select passwords and questions to verify their identity following guidelines that will make them difficult to guess.
- not disclose their passwords to anyone and avoid practices that may lead to them being exposed.
- change their passwords regularly, and as soon as possible after the password has been disclosed to another person, intentionally or accidentally, or when there is any indication of a possible system or password compromise; and must
- not bypass or disable any authentication process required to gain access to software, hardware, networks, information, or any other electronic resource owned or provisioned by the Mekong Institute.

The following documents containing more detail are relevant:

- IT User Access Policy
- Password Standard

5.3 Remote access

Access to MI's internal network from external networks and devices that are not under the control of the MI poses certain risks to the MI community. If the connection is not secure, there is a risk that unauthorized persons may be able to read data in transit that contain personal and confidential information. Furthermore, connections from malware-infected or compromised

sources or connections by unauthorized users may result in security breaches or damage to internal MI resources. Requirements to address such risks include:

- Only the official remote access software provided by IT unit may be used for remote access to the internal network.
- Remote access will be allowed for valid and confirmed needs only.
- Remote access users must have strong passwords for authentication and must ensure that devices used for remote access are secure.

5.4 Physical access

Physical security measures are required to prevent unauthorized physical access, damage and interference to MI's information and information processing facilities. Secure areas must be protected by appropriate entry controls in accordance with the identified level of acceptable risk and applicable IT standards, to ensure that only authorized persons are allowed access. Auditable records should be kept of access.

Any unit/dept that maintains electronic or paper-based MI's information is responsible for developing and implementing procedures to deny unauthorized access and ensure appropriate use to the best of its ability. Heads of units/departments are responsible for ensuring that procedures are in place to maintain access security and for educating their staff/members in these procedures. The printing of hard copies of confidential and personal information and documents is discouraged.

5.5 Internet and email usage

Use of the Internet and email poses certain risks to Mekong Institute. These include:

- Internet bandwidth is an expensive, shared, and limited resource. Its unrestricted usage may affect the speed of the Internet and, in extreme cases, the availability of Internet and email services, which is crucial for the continued, productive online research, operations and administrative activities of Mekong Institute.
- The Internet and email are channels continuously targeted by cybercriminals to gain access to information and IT resources within Mekong Institute network for malicious purposes.
- Unlawful use of the Internet and email by staff, visiting strategic partners and volunteers may lead to significant fines and reputational damage to Mekong Institute.

It is therefore necessary to have rules for managing the proper use of these services. These rules include requirements for:

- limiting the primary use of the Internet and email to operational, research and administrative purposes;
- regulating the shared use of the Internet;
- prohibiting use of the services for unlawful and malevolent activities; and
- preventing successful cyber-attacks.
- The IT will delete staff members' email accounts 30 days after their resignation.
- Monitoring -The Company reserves the right to monitor internet and network usage, including websites visited and content accessed, to ensure compliance with this policy and to maintain network security.

All users of Mekong Institute Internet and email services, telephony services and the SMS system must familiarize themselves with the Electronic Communications Policy.

5.6 Malware prevention

Mekong Institute will implement and maintain measures to prevent, detect and respond to malware attacks and infections. The IT unit staff responsible for these measures must familiarize themselves with the Malware Prevention Standard.

All users of the MI's network and IT resources must:

- ensure, as far as is reasonable, that their devices used to access the network are malware free.
- maintain a high level of awareness of malicious attempts, especially via email, that entice them to open malicious attachments, click on malicious links, or divulge personal information.
- use the Internet services in a responsible way so as not to introduce malware into the network or systems; and
- familiarize themselves with the Malware Prevention Guidelines for Users, which expands on practices that will facilitate compliance with the above requirements.

5.7 Service continuity

The IT unit provides service continuity through the deployment of redundant and resilient IT infrastructure. A second data Centre shall be established and will allow for the failover of critical services. This will reduce the impact of failures in the primary data Centre, as well as the likelihood of a complete failure of the IT unit infrastructure. Regular failover tests shall be executed to verify the correct configuration and adequacy of failover processes.

5.8 Backups

Backup copies of information and software are required to allow the continuation of related activities when such information or software on a device is damaged or destroyed, or the device is damaged, lost or stolen. This requires that:

- Data and software must be copied to a separate backup medium on a regular cycle for contingent use.
- Backed-up material should be kept disconnected from and in a location separate from the original system to protect it from the same hazards.
- The quality of backups and media and the ability to restore backed up data must be tested regularly.

The IT unit will ensure the backup of data and systems on all servers and the safe storage of such backups for recovery purposes.

Users are responsible for backing up the contents of their personal computers, as it is not done by the IT unit. Backups should include at least all data files created and maintained as part of their duties. Users are referred to guidelines in Methods to Perform Desktop/Laptop Backup for more information on backup strategy and available backup options. If required, external hard disks should be made available to users by their departmental/unit heads.

5.9 Network security

The MI network will be managed and controlled to ensure the availability of the network and the security of information in the network. Requirements include:

- physical protection of network equipment.
- control over equipment connecting to the network.
- authorized access to network equipment.
- secure design of the network.
- central management of DNS and IP addressing.
- additional security measures for protecting the server farms.
- control over external access to systems within the network; and
- controlled use of network management software.

A wireless network provides connectivity to the Internet to staff, consultants, volunteers and guests. Security requirements for the wireless network include:

- separation of the wireless network from the MI internal network;
- regulated expansion of the wireless network.
- different levels of access to different user groups.
- authenticated access by all user groups.
- device requirements for full access; and
- the right of Mekong Institute to monitor traffic flow under certain conditions.

5.10 Server security

All system administrators, including IT unit and non-IT unit staff, managing a computer server connected to MI local network system or global information networks must take reasonable security measures to secure their hosts. Requirements include:

- All servers connected to the network must be registered with IT unit.
- Operating system configurations should be in accordance with approved IT unit guidelines.
- Physical access to servers must be protected.
- Patch management must comply with IT unit defined standards.
- Local, dormant, and privileged accounts must be managed securely.
- Servers must be protected against malware.
- Server administrators are responsible to ensure regular backups of their servers.

5.11 Portable hardware and removable media

Portable hardware and removable storage include numerous types of hardware such as laptops, tablets, cell phones, flash drives, external hard disk drives, CDs, DVDs, etc. Users of such devices which contain institutional information are responsible to protect the information against unauthorized disclosure, modification or removal, loss or theft, regardless of who the owner of the device is. In this respect, the following is required:

- When making use of devices or media to store institutional information, users accept and take personal responsibility for the safe keeping of the devices or media and of any institutional information considered private, confidential or personal stored on such devices or media.
- When using devices or media, the user must ensure that all reasonable malware prevention has been taken.
- Devices and media containing confidential institutional information should be stored and disposed of securely.
- If a user loses, by accident or through theft, a device or media containing confidential MI information or personal information for which MI is responsible, it must be reported by email to the IT unit immediately.

5.12 Change management

Due to the extent and complexity of interdependencies within MI's information technology infrastructure, as well as the dependence of operational activities on its continuous availability, any additions, deletions or modifications of any component of the IT infrastructure must be carefully planned and monitored to reduce any potential negative impact of such changes on Mekong Institute.

Changes to hardware, software, operating systems, data and voice networks and applications, as well as direct changes to data and databases, are subject to the IT unit change management process which requires:

- identification and recording of significant changes.
- planning and testing of changes.
- assessment of potential impacts of such changes.
- a formal approval procedure for proposed changes.
- verification that predetermined requirements have been met.
- communication of change details to relevant parties.
- fall-back procedures to enable recovery from unsuccessful changes and unforeseen events; and
- provision of an emergency change process to enable quick and controlled implementation of change needed to resolve an incident.

5.13 System acquisition, development and maintenance

Information security is an integral part of information systems across their entire lifecycle. This includes systems acquired from a vendor, obtained through a license or subscription, customized or developed according to specific MI requirements, irrespective of where the system is hosted - whether on a server hosted by IT unit or a MI department or an external entity, on a personal user device, or in the cloud.

When new software is acquired or developed for use by a MI department or the wider MI community, the relevant system owner must:

- submit an assessment request to the IT Team for a risk assessment and to ensure compliance with relevant legislation and IT policy.
- log a request as early as possible to ensure that the software and hardware will comply with MI standards for development and security, and, if relevant, requirements to enable integration with other MI systems and infrastructure;
- follow formal procurement processes for the acquisition of the software.
- ensure the proper testing of the software in an isolated test environment.
- follow the formal IT unit change management procedure for its release into the MI environment;
- adhere to the Data Migration Standard when data is to be transferred from a current system to the new system.
- ensure that agreements with providers of solutions hosted in the cloud include that they will establish and maintain security measures to protect the service from fraudulent activity and unauthorized access, disclosure or modification of the software and transactions or information at rest and in transit.
- in addition, ensure that agreements with vendors who will process personal information on behalf of MI include a non-disclosure agreement, and the obligation to notify MI immediately should there be reasonable grounds to believe that such personal information has been unlawfully accessed, modified or acquired;
- when considering the adoption of a public cloud service to fulfil a system need, consider the risks and requirements related to the acceptable use of such services as stated in the IT Policy.

Responsibility for the maintenance of software depends on the software category and whether the software is categorized as being supported or unsupported by IT unit, as expounded in the IT policy on Software Use and Acquisition.

5.14 Privacy and confidentiality

Due care must be taken with the secure use, storage and sharing of personal information held by MI community. Such information must be collected, processed, stored and transferred among the MI and third parties, only in a manner that is consistent with MI ’s operational business

practices and policies.

5.15 Compliance with law and policy

The Mekong Institute IT infrastructure and facilities may only be used for authorized purposes. MI may from time to time, monitor or investigate usage of IT facilities and any person found using IT facilities or systems for unauthorized purposes, or without authorized access, may be subject to disciplinary and, where appropriate, legal proceedings. Furthermore, MI shall only permit the inspection and monitoring of operational logs by computer operations personnel and system administrators of the IT unit. Disclosure of information from such logs to officers of the law or to support disciplinary proceedings shall only occur when required by and consistent with law, there is reason to believe that a violation of law or of MI policy has taken place, or there are compelling circumstances.

To ensure that all software and licensed products used within the MI comply with the requirements of various acts relating to copyright, designs and patents, MI will carry out checks from periodically to ensure that only authorized products are being used and will keep a record of the results of those audits. Unauthorized copying of software or use of unauthorized products by staff, guests or consultants may be grounds for disciplinary and, where appropriate, legal proceedings.

It is unacceptable for anyone to use information resources to violate any Thai laws or MI's policies or perform unethical operations or business acts.

5.16 Security incidents reporting and management

All users have the responsibility to report immediately to the IT unit telephone ....., by email .....any observed or suspected security incidents where a breach of MI's security policies has occurred, and any security weaknesses in, or threats to, systems or services. This is required not only to prevent and resolve incidents, but also for the Mekong Institute to report certain security breaches in compliance with the Thai Data Act and the Cybercrimes Act.

The IT unit is responsible to:

- implement mechanisms to detect, report and analyze IT security incidents.
- implement and maintain incident management procedures to ensure a rapid and consistent response to incidents; and
- analyze incidents to mitigate the risk of future incidents and improve the incident management procedure.

5.17 Security risks

The IT unit is committed to appropriately manage information security risks related to the information, services and infrastructure under its control in alignment with MI's risk management framework. The identification of such risks is the responsibility of all staff of MI community, in particular, but not limited to, IT unit staff.

Likewise, the mitigation of such risks by all users through adherence to MI policies, responsible behavior and being security conscious plays a major role in reducing MI's risk exposure, and is the responsibility of all members of MI community.

6. Definitions

Administrators and technical staff	Individuals who design, manage and operate MI's electronic information resources, including, but not limited to, project managers, system designers, application programmers, application support staff, system administrators and user support staff.
Computer	A programable device that accepts information (in the form of digitalized data) and manipulates it for some result based on a program or sequence of instructions on how the data is to be processed, including, but not limited to, servers, workstations, desktop computers, laptop computers and electronic devices such as hubs, switches and routers.
Data	In this policy refers to information in digital form in databases, files, in transit via a network, etc, with no context or meaning attached.
IT infrastructure	The composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. It allows an MI to deliver IT solutions and services to its employees, partners etc
Managers	Individuals who have managerial responsibility for MI's organizational units, including, but not limited to Executive Director, Directors and heads of units and departments.
Personal computer (PC)	Any desktop computer or laptop computer provided by MI to one or more users for work or research purposes.
Security breach	Any incident that results in confirmed (not just potential) unauthorized access to computer data, applications, networks, or devices. It results in information being accessed without authorization.
Security incident	Any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information. This includes interference with information technology operation and violation of policy, laws, or regulations.
System owner	A manager who has the primary management responsibility for the functionality of a system, device or process, e.g. a head of department, director or senior line manager.
User(s)	Any person who accesses and uses MI's electronic information resources, including, but not limited to, employees, contract workers, independent contractors, temporary appointees, consultants, researchers etc

7. Roles and responsibilities

7.1 Users

Individuals who access and use MI's electronic information resources must:

(1) acquaint themselves with and adhere to the requirements of this policy and all policies, standards and guidelines referred to in this document.

(2) use all IT information resources (equipment, software, services, etc) to which access has been granted to them by Mekong Institute responsibly, with due care and in adherence to security policy and advisories.

(3) follow good security practices in selecting and using passwords.

(4) seek access to information only through Mekong Institute's authorization and access control process as embedded in MI IT unit infrastructure.

(5) follow good security practices to ensure that all devices used to access the IT infrastructure and systems are malware-free.

(6) use the services provided in a responsible way so as not to introduce malware into the network or systems.

(7) regularly backup MI data that is not stored centrally but on personal computers and any other electronic devices under their jurisdiction/ownership.

(8) ensure the physical protection of devices and media under their care and prevent unauthorized access to such devices and institutional information on such devices.

(9) not indiscriminately download or use software that is not supported or sanctioned by MI

(10) disseminate information to others only when authorized to do so, if governed by applicable delegations.

(11) comply with MI data policy and guidelines.

(12) comply with copyright and other applicable legislation listed in the Policy on Acceptable Use of Computing Resources; and

(13) report security incidents to the IT unit and retain evidence to assist with investigation should it be required.

7.2 Administrators and technical staff

Administrators and technical staff who design, manage and operate MI's electronic information resources must:

(1) define and implement access management processes for assigning and revoking user access codes and rights based on sound principles.

(2) implement data protection and access controls established by MI policies and standards.

(3) limit physical access to information assets.

(4) monitor compliance with information security standards.

(5) ensure that hardware (including, but not limited to, servers, PCs, network equipment, etc) and software are protected against malicious attacks and malware infections and are updated with appropriate security patches.

(6) define and implement procedures for the backup and recovery of information and systems.

(7) ensure the secure configuration of network equipment, devices, and servers.

(8) maintain ongoing internal audit processes (to the greatest technologically practical extent), which record system activity such as logins, file accesses, and security incidents;

(9) carefully plan and follow the defined change management procedures when making changes to hardware, software, operating systems, networks and applications.

(10) ensure processes are in place for the detection of security violations.

(11) take appropriate responsive action to limit the impact of events that pose a threat to security.

7.3 IT unit Management

The IT manager and deputies are responsible for ensuring that relevant IT staff take up their responsibilities to implement tasks attributed to the IT unit in this policy. These include:

(1) maintenance and management of appropriate controls and security measures.

(2) the identification, assessment, and monitoring of security risks.

(3) communication with users on policy requirements, security issues and threats, and providing security advice; and

(4) efficient management of security incidents. Appendix A–Diagram: The policy and its associated documents.