

# **ACTUARIAL SERVICES AND RISK MANAGEMENT SECTOR**

# **INTERNAL SERVICES**

Volume 16

OFFICE OF THE SENIOR VICE-PRESIDENT - ACTUARIAL SERVICES AND RISK MANAGEMENT SECTOR
CORPORATE INFORMATION SECURITY DEPARTMENT
PROJECT MANAGEMENT TEAM FOR RISK MANAGEMENT



# LIST OF SERVICES

INTERNAL SERVICES	PAGE
ACTUARIAL SERVICES AND RISK MANAGEMENT SECTOR	
OFFICE OF THE SENIOR VICE-PRESIDENT – ACTUARIAL SERVICES	
AND RISK MANAGEMENT SECTOR	3
Receiving Documents Requiring Action	3-4
CORPORATE INFORMATION SECURITY DEPARTMENT	5
1. Information Security Incident Management (Highly Technical)	5
2. Information Security Incident Management (Simple)	6
3. Monitoring of Information Security Policy and Protocols	7-9
4. Handling of Complex Information Security Concerns	10
5. Handling of Data Privacy Concerns	
6. Handling of Highly Information Security Concerns	13
7. Handling of Simple Information Security Concerns	
8. Information Security Incident Management (Complex)	15
9. Information Security Policy and Protocols Development	16-17
10. Retrieval of Back-up Tapes	18
11. Retrieval Tape Vault Storage	19
12. Safekeeping of Back-up Tapes	20-21
13. Safekeeping Tape Vault Storage	22
PROJECT MANAGEMENT TEAM FOR RISK MANAGEMENT	23
1. Issuance of Risk Assessment Certification (RAC) for New	
And Amended Programs, Projects, and Policies	23-24



# OFFICE OF THE SENIOR VICE-PRESIDENT - ACTUARIAL SERVICES AND RISK MANAGEMENT SECTOR

#### 1. RECEIVING DOCUMENTS REQUIRING ACTION

This is specific to simple inquiries that can be addressed immediately, i.e., inquiry on benefits, accreditation. standards of care policy

Office/Division	Office of the Senior Vice Presodent - Actuarial Services and Risk Management Sector					
Classification	Simple	Simple				
Type of	G2C; G2B; G2G					
Transaction						
Who may avail:						
<b>CHECKLIST OF RE</b>	EQUIREMENTS WHERE TO SECURE					
None		None				
CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE (Position of Supervisor)		
1. Send Memorandum	1.1. Receive memorandum through personal service	None	2 minutes	Administrative staff		
	1.2 Log and upload electronic copy in registry	None	3 minutes	Administrative staff		
	1.3 Forward memorandum	None	1 minute	Administrative staff		
	1.4. Review memorandum as to required action from the Senior Vice President	None	3-15 minutes	Executive Assistant		
	1.5. Prepare recommendation on the appropriate course of action of the Senior Vice President, or prepare draft reply, whichever is applicable	None	3-15 minutes	Executive Assistant		
	<ul><li>1.6 Evaluate the memorandum to determine the proper course of action which may be any of the following:</li><li>(1) instruct to prepare reply or initiate conduct of study;</li></ul>	None	15 minutes	Senior Vice President		



TOTAL	None	2 days	
1.8 Release the reply-memorandum, report, or endorsement to sender; and appropriate offices, if applicable	None	3 minutes	Administrative staff
1.9 Review and sign the reply, report, endorsement, or memo which apprises the sender of the course of action taken and the expected TAT	None	10 minutes	Senior Vice President
1.8 Comply with the instruction of the Senior Vice President	None	15 minutes	Executive Assistant
information, or seek clarification  1.7. Instruct the Executive Assistant on the appropriate course of action	None	5 minutes; however actuarial reports and studies may take longer depending on the nature of the study	Senior Vice President
<ul><li>(2) forward to PMT-RM/ CISD/ OA;</li><li>(3) forward to the concerned offices outside the sector to request data or information;</li><li>(4) return to sender to ask for additional data or</li></ul>			



# **CORPORATE INFORMATION SECURITY DEPARTMENT**

### 1. INFORMATION SECURITY INCIDENT MANAGEMENT (HIGHLY TECHNICAL)

Concerns the handling of incidents reported

Office/Division	Corporate Information Security Department (InfoSec)			
Classification	Highly Technical			
Type of Transaction	G2G - Government to Government			
Who may avail:	Employees who experienced or discovered a	n information	on security incident	
CHECKLIST C	OF REQUIREMENTS		WHERE TO	SECURE
Incident report (IR) form (including pro	oofs or pieces of evidence) (1 Original and			
Digital Copy Accepted)		Attached as	Annex A to Office	Order No. 0086-2015
		FEES TO	PROCESSING	
CLIENT STEPS	AGENCY ACTION	BE PAID	TIME	PERSON RESPONSIBLE
	1.1 Receive the incident report	None	5 minutes	
	1.2 Update the incidents register	None	5 minutes	
1.The employee/ initiator properly	1.3 Review the incident report and classify	None	1 hour	
accomplishes the IR Form	1.4 Set meeting and convene, officers, and			
a. Attach pertinent documents to	employees involved in the incident	None	2 days	
support the report	1.5 Facilitate the resolution of the incident	None	5 days	
b. Submit the report to InfoSec (walk-	1.6 Document the incidents as well as the			
in, email, direct message)	agreements	None	1 day	Information Systems
	2.1. Close the incident	None		Analyst II, InfoSec
2. Expect a notification from the	2.2 Monitor the agreements.	None	5 minutes	Information Technology
InfoSec Operations Division	2.3 Perform assessment if warranted.	None	5 minutes	Officer III, InfoSec
			8 days, 1 hour, 15	
	Total	None	mins	



# 2. INFORMATION SECURITY INCIDENT MANAGEMENT (SIMPLE)

Concerns the handling of incidents reported

concerns the naming of melacitis reported					
Office/Division	Corporate Information Security Department (InfoSec)				
Classification	Simple	Simple			
Type of Transaction	G2G - Government to Governm	nent			
Who may avail:	Employees who experienced o	r discovered a	n information secu	rity incident	
CHECKLIST OF REQUIRE	MENTS		WHERE TO	O SECURE	
Incident report (IR) form (including proofs or pie	eces of evidence) (1 Original				
and Digital Copy Accepted)		Attached as A	nnex A to Office C	order No. 0086-2015	
		FEES TO BE	PROCESSING		
CLIENT STEPS	AGENCY ACTION	PAID	TIME	PERSON RESPONSIBLE	
1. The employee /initiator properly					
accomplishes the IR Form	1. Receive the incident report	None	5 minutes		
2. Attach pertinent documents to support the	2. Update the incidents				
report	register	None	5 minutes		
3. Submit the report to InfoSec (walk-in, email,	3. Review the incident report				
direct message)	and classify	None	1 hour		
4. Expect a notification from the InfoSec	Information Systems Analys				
Operations Division	4. Address the incident None II, InfoSec				
	TOTAL	None	3 hours, 10 mins		



#### 3. MONITORING OF INFORMATION SECURITY POLICY AND PROTOCOLS

Concerns with overseeing the implementation of security controls and measures, together with other Corporate units tasked to monitor and enforce them.

Office/Division	Corporate Information Security Department (InfoSec)				
Classification	Highly Technical				
Type of Transaction	G2G - Government to Government				
	Business Process Units (BPUs), which require secure corporate information systems (people, process and technology).				
	The BPUs in consultation and coordination with Corporate Ir information security risks.	nformati	on Security Department ide	ntify and assess	
Who may avail:	The Corporate Information Security Department, both as a BPU and as a responsible office for information security identify and assess information security risks				
	CHECKLIST OF REQUIREMENTS WHERE TO SECURE			E	
		Reported through Risk Information Management			
Anyone of the following:		-	(RIMS)/For manual copy, RI		
Risk information sheet (RIS)	(1 Original Copy);	attachn	nent of PhilHealth-SOP-01-0	2-002	
Feedback through email/Re	port from Information Security Awareness Officer (1				
Original copy)		No pres	scribed form		
		Receive	d and assessed incident rep	ort by Security	
		-	ons Division (OpSec) of Corp	porate	
	rity Incident Report (1 Original Copy); or	Informa	ation Security Department		
Audit Findings and Recomm	nendations Referred by Internal Audit Group and (Internal				
Audit Group/COA) (1 Original Copy)		Referre	d by Internal Audit Group a	nd COA	
	FEES				
	TO BE PERSON				
CLIENT STEPS	AGENCY ACTION	PAID	PROCESSING TIME	RESPONSIBLE	
1. Implement information	1. Monitor policy compliance through the following			Information	
security controls and	avenues:	None	1/2 day	Systems Analyst	



measures:	a. Security Education, Training and Awareness (SETA)			II, InfoSec
a. RIS or RIMS;	activity gathers feedback on policy implementation;			Information
b. Feedback through	b. Incident assessment results and self-assessment;			Systems Analyst
email/Report from	c. Internal Audit Group's audit findings with its			III, InfoSec
Information Security	recommendations relating to Information Security and Data			
Awareness Officer;	Privacy;			
c. Assessed Information	d. Audit Findings and Recommendations (Internal Audit			
Security Incident Report;	Group/COA)			
or				
d. Audit Findings and				
Recommendations				
(Internal Audit				
Group/COA)				
				Information
				Systems Analyst
				II, InfoSec
	2. Reassess information security risks and their			Information
	corresponding controls and measures (Guidelines, Policy			Systems Analyst
	and Standard Operating Procedure)	None	1 day	III, InfoSec
				Information
	3. Revises the corresponding controls and measures			Systems Analyst
	(Guidelines, Policy and Standard Operating		18days (Initial/Final	II, InfoSec
	Procedures)based on the results of the reassessment and in		Review of Concerned	Information
	accordance with PhilHealth-SOP-01-01-001 (Policy		Offices/Approval and	Systems Analyst
	Formulation Process) and Office Order 0060, series of 2015	None	Signature of Sector Heads	III, InfoSec



(Creation, Revision and Use of Standard Operating			Information
Procedure)			Technology
			Officer III,
			InfoSec
			Senior Manager,
			InfoSec
Total	None	20 days	



#### 4. HANDLING OF COMPLEX INFORMATION SECURITY CONCERNS

Concerns with managing information security concerns across the PhilHealth Organization. It basically covers the formulation of security measures and controls based on the results of the identified and assessed risks on programs and projects.

Office:	Corporate Information Security Department (InfoSec)					
Classification:	Complex					
Type of Transaction:	Internal Service (G2G)					
	Business Process Units (BPUs), which require secure corporate information systems (people, process and technology).					
	The BPUs in consultation and coordination with Corporate Information Security Department identify and assess information security risks.					
	The Corporate Information Security Dep	artment, bot	h as a BPU and as a resp	onsible office for information		
Who May Avail:	security identify and assess information security risks					
CHECKLIST O	IST OF REQUIREMENTS WHERE TO SECURE					
None		None				
		FEES TO BE				
CLIENT STEPS	AGENCY ACTION	PAID	PROCESSING TIME	PERSON RESPONSIBLE		
1. Send query/feedback via	1.1. Received letter/memo.		5 minutes			
letter/memo to InfoSec.	1.2. Assessed received letter/memo.		4 hours	Clerk III, InfoSec		
	1.3. Evaluate and prepare response memo.		4 days	Senior Manager, InfoSec Information Technology		
	1.4. Review draft response memo and provide comments, if any.		1 day	Officer III, InfoSec Information Systems Analyst		
	1.5. Finalize reply, if with comments.		1 day	III, InfoSec		
	1.6. Sign finalized response letter.	2 hours Information Systems A				
	1.7. Release response letter to client.					
	TOTAL:		6 days 6 hours and 10 minutes			



#### 5. HANDLING OF DATA PRIVACY CONCERNS

Handling of concerns involving processing of personal information and compliance with the Data Privacy Act

Trunuling of concerns involving processing of perso	onai injormation ana compnance with the Data F	TIVULY AL	-L		
Office:	Corporate Information Security Department (Ir	Corporate Information Security Department (InfoSec)			
Classification:	Highly Technical				
Type of Transaction:	Internal Service (G2G)				
	Employees' and external stakeholder's concern	s on prol	pable violation of	the Data Privacy	
Who May Avail:	Act				
CHECKLIST OF R	KLIST OF REQUIREMENTS WHERE TO SECURE				
Submission/endorsement of documents, electron	ic mail, and other forms of reporting data	Attache	d as Annex A to C	Office Order No.	
privacy concerns	0086-2015				
		FEES			
		TO BE	PROCESSING	PERSON	
CLIENT STEPS	AGENCY ACTION	PAID	TIME	RESPONSIBLE	
1. The employee/external stakeholder properly	1. Receipt of the report/concern from Clerk III			Clerk III	
submits/endorses documents, electronic mail,					
and other forms of reporting data privacy				Information	
concerns.				Systems Analyst II	
2. Attach evidences to support the	2. Evaluation and assignment of the			Information	
report/concern.	report/concern to the appropriate			Systems Analyst	
	Information Systems Analyst		5 minutes		
				Information	
				Technology	
			4 hours	Officer III	
3. Submit the report/concern to InfoSec through	3.1. Conduct of technical assessment,				
established means of communication (walk-in,	research and/or meetings with relevant				
email, snail mail, business correspondence).	Business Process Owners (BPOs) in aid of	Nieres	1.0 -1		
	addressing the report/concern.	None	16 days		



InfoSec Data Privacy Division.	Manager for approval  TOTAL:	5 minutes  20 days, 4 hours, 10 mins	
4. Expect a notification/response from the	4. Submission to the Office of the Senior		
	3.3. Technical review of documentation that addressed the report/concern.	2 days	
	agreements that addressed the report/concern.	2 days	
	3.2. Crafting of memoranda and/or other forms of documentation as well as the		



#### 6. HANDLING OF HIGHLY TECHNICAL INFORMATION SECURITY CONCERNS

Concerns with managing information security concerns across the PhilHealth Organization. It basically covers the formulation of security measures and controls based on the results of the identified and assessed risks on programs and projects.

Office:	Corporate Information Security Department (InfoSec)					
Classification:	Highly Technical					
Type of Transaction:	Internal Service (G2G)					
	Business Process Units (BPUs), which require secure corporate information systems (people, process and technology).					
	The BPUs in consultation and coordination with Corporate Information Security Department identify and assess information security risks.					
	The Corporate Information Security Department, both as a BPU and as a responsible office for information					
Who May Avail:	security identify and assess information security risks					
CHECKLIST O	KLIST OF REQUIREMENTS WHERE TO SECURE					
None		None				
		FEES TO BE				
CLIENT STEPS	AGENCY ACTION	PAID	PROCESSING TIME	PERSON RESPONSIBLE		
1. Send query/feedback via	1.1. Received letter/memo.		5 minutes			
letter/memo to InfoSec.	1.2. Assessed received letter/memo.		1 day	Clerk III, InfoSec		
	1.3. Evaluate and prepare response memo.		15 days	Senior Manager, InfoSec Information Technology		
	1.4. Review draft response memo and provide comments, if any.		2 days	Officer III, InfoSec Information Systems Analysi		
	1.5. Finalize reply, if with comments.		2 days	III, InfoSec		
	1.6. Sign finalized response letter.		2 hours	Information Systems Analyst		
	1.7. Release response letter to client.					
	TOTAL:		20 days 2 hours and 10 minutes			



#### 7. HANDLING OF SIMPLE INFORMATION SECURITY CONCERNS

Concerns with managing information security concerns across the PhilHealth Organization. It basically covers the formulation of security measures and controls based on the results of the identified and assessed risks on programs and projects

Office/Division	Corporate Information Security Department (InfoSec)
Classification	Simple
Type of Transaction	Internal Service (G2G)
Who may avail:	Business Process Units (BPUs), which require secure corporate information systems (people, process, and technology).

CHECKLIST OF REQUIREMENTS	WHERE TO SECURE
None	None

CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE (Position of Supervisor)
1. Send query/feedback via letter/memo to InfoSec.	1.1. Received letter/memo.		5 minutes	
	1.2. Assessed received letter/memo.		3 hours	
	1.3. Evaluate and prepare response memo.		1 day	
	1.4. Review draft response memo and provide comments, if any.	None	1 day	Clerk III, InfoSec Senior Manager, InfoSec Information Technology Officer III, InfoSec Information Systems Analyst III, InfoSec Information Systems Analyst II, InfoSec
	1.5. Finalize reply, if with comments.		1 day	
	1.6. Sign finalized response letter.		1 day	
	1.7. Release response letter to client.		5 minutes	
	TOTAL	None	3 days 4 hours and 15 minutes	



# 8. INFORMATION SECURITY INCIDENT MANAGEMENT (COMPLEX)

Concerns the handling of incidents reported

concerns the nanding of incluents rep	0,124					
Office/Division Corporate Information Security Department (InfoSec)						
Classification	Complex					
Type of Transaction	G2G - Government to Government					
Who may avail:	Employees who experienced or discovered a	an informati	on security incident			
CHECKLIST C	OF REQUIREMENTS		WHERE TO	SECURE		
Incident report (IR) form (including pro Digital Copy Accepted)	pofs or pieces of evidence) (1 Original and	Attached as	s Annex A to Office	Order No. 0086-2015		
CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE		
	1.1 Receive the incident report	None	5 minutes			
	1.2 Update the incidents register	None	5 minutes			
1.The employee/ initiator properly	1.3 Review the incident report and classify	None	1 hour			
accomplishes the IR Form	1.4 Set meeting and convene, officers, and					
a. Attach pertinent documents to	employees involved in the incident	None	1 day			
support the report	1.5 Facilitate the resolution of the incident	None	2 days			
b. Submit the report to InfoSec (walk-	1.6 Document the incidents as well as the					
in, email, direct message)	agreements	None	4 hours	Information Systems		
	2.1. Close the incident	None	5 minutes	Analyst II, InfoSec		
2. Expect a notification from the	2.2 Monitor the agreements.	None		Information Technology		
InfoSec Operations Division	2.3 Perform assessment if warranted.	None	5 minutes	Officer III, InfoSec		
	Total	None	3 days, 5 hours, 15 mins			
	Total	None	T2 1111112			



#### 9. INFORMATION SECURITY POLICY AND PROTOCOLS DEVELOPMENT

Concerns with managing information security across the PhilHealth Organization through corporate policy development. It basically covers the formulation of security measures and controls based on the results of the identified and assessed risks, and assessed security incidents.

, ,	is and controls based on the results of the identified and	ussesseu	Tisks, and assessed security	meraents.		
Office/Division	Corporate Information Security Department (InfoSec)					
Classification	Highly Technical					
Type of Transaction	G2G - Government to Government					
	Business Process Units (BPUs), which require secure corporate information systems (people, process and technology).					
	The BPUs in consultation and coordination with Corporate Information Security Department identify and assess information security risks.					
	The Corporate Information Security Department, both a	as a BPU	and as a responsible office f	or information		
Who may avail:	security identify and assess information security risks		·			
CHECKLIST OF REQUIREMENTS WHERE TO SECURE						
		Reporte	ed through Risk Information	Management		
Anyone of the following:		System (RIMS)/For manual copy, RIS Form is an				
Risk information sheet (RIS) (1 0	Original Copy);	attachn	nent of PhilHealth-SOP-01-0	2-002		
Feedback through email/Report	t from Information Security Awareness Officer (1					
Original copy)		No pres	cribed form			
		Receive	d and assessed incident rep	ort by Security		
		Operations Division (OpSec) of Corporate Information				
Assessed Information Security I	ncident Report (1 Original Copy); or	Security	Department			
Audit Findings and Recommend	lations Referred by Internal Audit Group and (Internal					
Audit Group/COA) (1 Original Co	ору)	Referred by Internal Audit Group and COA				
		FEES				
		TO BE		PERSON		
CLIENT STEPS	AGENCY ACTION	PAID	PROCESSING TIME	RESPONSIBLE		
1. Identify information security	1. Assessed received:			Information		
risk/ information security	a. RIS;	None	1/2 day	Systems Analyst		



issue/ concern and report	b. Feedback through email/Report from Information		•	II, InfoSec
through any of the following:	Security Awareness Officer;			Information
a. RIS or RIMS;	c. Assessed Information Security Incident Report; or			Systems Analyst
b. Feedback through	d. Audit Findings and Recommendations (Internal			III, InfoSec
email/Report from Information	Audit Group/COA)			
Security Awareness Officer;				
c. Assessed Information				
Security Incident Report; or				
d. Audit Findings and				
Recommendations (Internal				
Audit Group/COA)	2. Develop information security controls and measures			Information
	(Guidelines, Policy and Standard Operating Procedure)			Systems Analyst
	in accordance with PhilHealth-SOP-01-01-001 (Policy		17 1/2 days (Initial/Final	II, InfoSec
	Formulation Process) and Office Order 0060, series of		Review of Concerned	Information
	2015 SOP (Creation, Revision and Use of Standard		Offices/Approval and	Systems Analyst
	Operating Procedure)	None	Signature of Sector Heads)	III, InfoSec
				Information
				Systems Analyst
				II, InfoSec
				Information
				Systems Analyst
				III, InfoSec
				Information
				Technology
				Officer III,
	3. Communicate information security controls and			InfoSec
	measures through Outlook and SETA (Guidelines,			Senior Manager,
	Policy and Standard Operating Procedure		1 day	InfoSec
	Total	None	20 days	



#### 10. RETRIEVAL OF BACK-UP TAPES

Concerns the tape vault storage retrieval of back-up tapes

Office:	Corporate Information Security Department (InfoSec)						
Classification:	Simple						
Type of Transaction:	Internal Service (G2G)						
Who May Avail:	Information Technology Management Departm	ent					
CHECKLI	ST OF REQUIREMENTS		WHERE TO	SECURE			
Consolidated Vault Inventory List (2 Original Copies)  Vault access request/ endorsement of back-up tape for storage (2 Original			Information Technology Management Department / Information Management Sector Information Technology Management Department /				
Approved withdrawal of tapes request (2 Original Copies)			Information Management Sector Information Technology Management Department / Information Management Sector				
		FEES TO BE					
CLIENT STEPS	AGENCY ACTION	PAID	PROCESSING TIME	PERSON RESPONSIBLE			
1. Prepare letter request / back-	1.1. Receive and log all letter request.		5 minutes	Clerk III, InfoSec			
up tape retrieval.	1.2. Coordinate with PRID on the availability of service vehicle to Media Library.		3 days	Senior Manager, InfoSec Information Technology			
2. Endorse approved letter	2.1 Identify back-up tapes for retrieval.		4 hours	Officer III, InfoSec			
request to CISD	2.2. Update Vault Inventory List		2 hours	Information Systems Analyst			
	2.3. Retrive back-up tapes.		15 minutes	II, InfoSec			
	2.4. Ensure that vaults and Media Library are locked.	None 5 minutes		Information Systems Analyst III, InfoSec			
	TOTAL:		3 days, 6 hours, 25 mins				

<sup>\*</sup>subject to approval of blanket CPO regarding Authority to Travel to Media Library (submitted every first month of the year) and availability of service vehicle



#### 11. RETRIEVAL TAPE VAULT STORAGE

Concerns the tape vault storage retrieval of back-up tapes

concerns the tupe vault storage ret						
Office/Division	Corporate Information Security Department (InfoSec)					
Classification	Simple					
Type of Transaction	G2G - Government to Government					
Who may avail:	Information Technology Management Dep	partment				
CHECKLIST OF REQUIREMENTS		WHERE TO SE	CURE			
Consolidated Vault Inventory List (2	2 Original Copies)		echnology Manago Nanagement Secto	ement Department / r		
Vault access request/ endorsement Copies)	t of back-up tape for storage (2 Original		echnology Manago Nanagement Secto	ement Department / r		
Approved withdrawal of tapes request (2 Original Copies)		Information Technology Management Department / Information Management Sector				
CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE		
1. Prepare letter request / back-up tape retrieval.	1. Receive and log all letter request.	None	5 minutes			
2. Endorse approved letter request to CISD	2. Identify back-up tapes for retrieval.	None	5 minutes			
	3. Update Vault Inventory List	None	5 minutes			
	4. Coordinates with codes custodian and			Clerk III, InfoSec		
	physical key custodian.	None	5 minutes	Information Systems Analyst		
	5. Retrieve back-up tapes.	None	5 minutes	III, InfoSec		
	Total	None	25 minutes			



#### 12. SAFEKEEPING BACK-UP TAPES

Concerns the tape vault storage, safekeeping of back-up tape

concerns the tape vault storage, sajek	ceping of back ap tape					
Office:	Corporate Information Security Department (InfoSec)					
Classification:	Simple					
Type of Transaction:	Internal Service (G2G)					
Who May Avail:	Vho May Avail: Information Technology Management Department					
CHECKL	ST OF REQUIREMENTS	WHERE TO SECURE				
		Informati	on Technology M	anagement		
Consolidated Vault Inventory List (2 O	riginal Copies)	Departme	ent / Information	Management Sector		
		Informati	on Technology M	anagement		
Vault access request/ endorsement of	back-up tape for storage (2 Original Copies)	Departme	ent / Information	Management Sector		
	Informati	on Technology M	anagement			
Approved withdrawal of tapes request (2 Original Copies)			ent / Information	Management Sector		
		FEES TO	PROCESSING			
CLIENT STEPS	AGENCY ACTION	BE PAID	TIME	PERSON RESPONSIBLE		
1. Document/Label Back-up tapes.	1.1. Receive, encodes and prepares Vault Inventory					
	List based on Endorsement Letter from ITMD.		5 minutes			
	1.2. Coordinate with PRID on the availability of			Clerk III, InfoSec		
	service vehicle to Media Library.		3 days	Senior Manager,		
2. Prepare consolidated list of	2. Validates the endorsed inventories. Checks the			InfoSec		
inventories/back-up tapes for	completeness and documentation of the endorsed			Information		
transport and storage.	inventories/back-up tapes.		4 hours	Technology Officer III,		
3. Prepare memorandum to				0,		
•	3.1. Receives back-up tapes based on Vault			InfoSec		
Department Manager CISD.	Inventory List.		15 minutes			
•	Inventory List.  3.2. Signs and completes signatories of Vault	_		InfoSec Information Systems Analyst II, InfoSec		
•	Inventory List.		15 minutes 15 minutes	InfoSec Information Systems		



3.4. Ensure that vaults and Media Library are					
locked.		5 minutes			
		3 days, 4 hours,			
TOTAL:		45 mins			
*subject to approval of blanket CPO regarding Authority to Travel to Media Library (submitted every first month of the year) and availability of service vehicle					

<sup>\*</sup>subject to approval of blanket CPO regarding Authority to Travel to Media Library (submitted every first month of the year) and availability of service vehicle



#### 13. SAFEKEEPING TAPE VAULT STORAGE

Concerns the tape vault storage, safekeeping of back-up tape

concerns the tupe vault storage, sajek	ceping of suck up tupe				
Office/Division	Office/Division Corporate Information Security Department (InfoSec)				
Classification	Highly Technical				
Type of Transaction	G2G - Government to Government				
Who may avail:	Information Technology Management Department				
CHECKLIST OF REQUIREMENTS		WHERE TO	) SECURE		
		Informatio	n Technology M	anagement	
Consolidated Vault Inventory List (2 O	riginal Copies)	Departme	nt / Information	Management Sector	
		Informatio	n Technology M	anagement	
Vault access request/ endorsement of	back-up tape for storage (2 Original Copies)	Departme	nt / Information	Management Sector	
		Informatio	on Technology M	anagement	
Approved withdrawal of tapes request	(2 Original Copies)	Departme	nt / Information	Management Sector	
		FEES TO	PROCESSING		
CLIENT STEPS	AGENCY ACTION	BE PAID	TIME	PERSON RESPONSIBLE	
	1. Receive, encodes and prepares Vault Inventory				
1. Document/Label Back-up tapes.	List based on Endorsement Letter from ITMD.	None	5 minutes		
2. Prepare consolidated list of	2. Validates the endorsed inventories. Checks the				
inventories/back-up tapes for	completeness and documentation of the endorsed				
transport and storage.	inventories/back-up tapes.	None	5 minutes		
3. Prepare memorandum to	3. Receives back-up tapes based on Vault Inventory				
Department Manager CISD.	List.	None	5 minutes		
	4. Signs and completes signatories of Vault				
	Inventory List by ITMD Representative and Guard				
	on duty	None	5 minutes		
	5. Coordinates with codes custodian and physical			Clerk III, InfoSec	
	key custodian.	None	5 minutes	Information Systems	
	6. Deposit/Store back-up tapes	None	5 minutes	Analyst III, InfoSec	
	Total	None	30 minutes		



#### PROJECT MANAGEMENT TEAM FOR RISK MANAGEMENT

#### 1. ISSUANCE OF RISK ASSESSMENT CERTIFICATION (RAC) FOR NEW AND AMENDED PROGRAMS, PROJECTS AND POLICIES

As part of Completed Staff Work (CSW) requirements, the Risk Assessment Certification is issued to ensure the risk management process is carried out and applied by the proponent in the course of developing new and amended programs, projects, and policies.

Office/Division	Project Management Team for Risk Management (PMT-RM)					
Classification	Complex					
Type of Transaction	G2G- Government to Government					
Who may avail:	All PhilHealth Head Offices (Proponent)					
CHECK	LIST OF REQUIREMENTS		WHERE T	O SECURE		
Draft program, project, or policy	(1 photocopy)	Proponer	nt Office			
Risk Self-Assessment Questionna	aire (1 original)	Proponer	nt Office			
Risk Information Sheet (RIS) (1 p	hotocopy)	Proponer	nt Office			
Risk Registry (1 photocopy)		Proponer	nt Office			
		FEES TO				
CLIENT STEPS	AGENCY ACTION	BE PAID	PROCESSING TIME	PERSON RESPONSIBLE		
1. Submit required documents						
for initial assessment and	1.1. Receive required documents and check for					
verification	completeness	None				
	1.2. Record documents in logbook	None		Clerk/ Administration		
	1.3. Endorse documents to technical staff of			Services Assistant C (ASA C),		
	PMT-RM	None	2 hours	PMT-RM		
	1.4 Check documents contents for					
	completeness	None				
1.5 Review, evaluate and validate submitted						
	documents					
	1.6 Sign Risk Self-Assessment Questionnaire					
	(RSAQ)	None		Project Development Officer		
	1.7 Prepare certification	None	4 working days	III, PMT-RM		



\	None None		Senior Manager, PMT- RM Clerk/ Administration
2.2. Release signed RSAQ and RAC	None		Services Assistant C (ASA C), PMT-RM
TOTAL		4 Days, 1 Hour and 15 Minutes	