



HANBRIDGE INSTITUTE

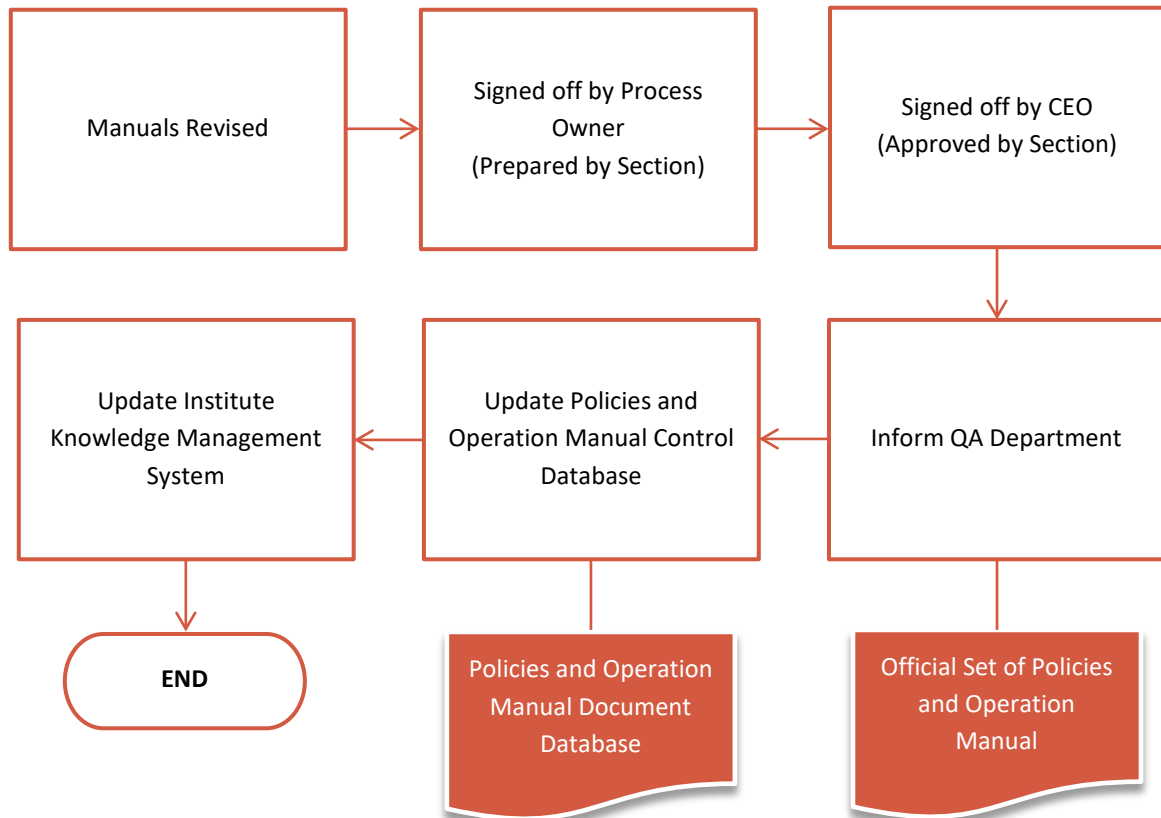
**OPERATION MANUAL**

**OM-0406-C2.5.1-05**

**CONFIDENTIALITY AND SECURITY OF INFORMATION**

## 1. Document Control Policy



One of the Institute’s Controlled Documents will include the Official Set of Policies and Operation Manuals (“Manuals”) that must be endorsed and approved by the Chairman of PMER Committee prior to its release to any stakeholders. Any revisions to the Manuals must be documented / reflected in the Revision History (Item 2) of this Manual and also in the Policy and Operation Manual Document Control Database. The flowchart below captures the approval process and their respective supporting documents.



## 2. Revision History

Version	Description	Effective Date
00	Initial Release	27 March 2017
01	<ul style="list-style-type: none"> <li>Changed Criterion to 2.5.1</li> </ul>	15 June 2017
02	<ul style="list-style-type: none"> <li>Added new section 8 on review of process</li> <li>Changed section 3 on setting up of email account to be done by HR Executive</li> </ul>	28 February 2018
03	<ul style="list-style-type: none"> <li>Updated Document Signatory List</li> </ul>	27 November 2018
04	<ul style="list-style-type: none"> <li>Amended Department Coding from "0409" to "0406"</li> <li>Removed General Information header and box</li> <li>Removed signing date from Document Signatory List</li> <li>Amended Prepared By Name</li> <li>Amended Approved By Name</li> <li>Amended "Acknowledgement Form for Access Rights" to "Access Rights Acknowledgement Form" in Manual</li> <li>Removed "Confidentiality and Non-Disclosure Pact" from Manual</li> <li>Amended "Employee Issuance and Clearance Form" to "Issuance and Exit Clearance Form" in Manual</li> <li>Amended "Head of Department/Principal" to "Management" in Point 5.4</li> <li>Amended "Designated Independent Internal Auditor" to "Independent Internal Process Auditor" in Point 8.1</li> </ul>	17 July 2019
05	<ul style="list-style-type: none"> <li>Changed logo</li> <li>Amended "School" to "Institute" throughout the manual</li> </ul>	18 March 2020

## 3. Document Signatory List

Responsibility	Name	Title	Signature
Prepared by	Elaine Ng	HR Executive	
Approved by	Alan Go	Chairman of PMER Committee	

Write-up: Process Details	Documentation & Responsibility
<p><b>1. Restricted Access Rights</b></p> <p>1.1 The Institute has various mechanisms in place to ensure that proper access rights are granted to relevant staffs at the right level so as to protect the confidentiality and security of the Institute. The various procedures are as follows: -</p> <ul style="list-style-type: none"> <li>• Acknowledgement of Personal Data Protection Policy</li> <li>• Setting up / Removal of E-mail Accounts</li> <li>• Computerized Institute Management System</li> </ul> <p>1.2 The <a href="#">Confidentiality and Security Policy</a> can be found in the Institute’s Policy Manuals and is communicated to employees through the <a href="#">Staff Handbook</a>.</p> <p>Note: Staff are to sign and complete the <a href="#">Access Rights Acknowledgement Form</a> (usually part of the contract) as part of the Institute’s Confidentiality and Security of Information process.</p>	<p><a href="#">Staff Handbook</a> (HR Executive)</p> <p><a href="#">Acknowledgement Form for Access Rights</a> (HR Executive)</p>
<p><b>2. Acknowledgement of Personal Data Protection Policy</b></p> <p>2.1 Staff are to read and understand the contents of the <a href="#">Personal Data Protection Policy</a>, and sign on the <a href="#">Acknowledgement of Personal Data Protection Statement</a> as acknowledgement.</p> <p>2.2 Staff will sign the statement when they are selected for employment.</p> <p>2.3 Students will sign the acknowledgement of the Personal Data Protection Policy within the <a href="#">Student Application Form (Local &amp; International)</a>, when they enroll into the Institute.</p>	<p><a href="#">Acknowledgement of Personal Data Protection Statement</a> (HR Executive)</p> <p><a href="#">Student Application Form (Local &amp; International)</a> (Course Registrar)</p>
<p><b>3. Setting up of Email Account</b></p> <p>3.1 Upon signing of the employment letter, the <a href="#">HR Executive</a> will proceed to create an email account for the new staff. A unique email account will be assigned, together with the Password and Quota of the Account.</p> <p>3.2 The <a href="#">HR Executive</a> will then pass on this account information to the new staff accordingly.</p>	
<p><b>4. Staff Resignation: Removal of E-mail Account</b></p> <p>4.1 The <a href="#">HR Executive</a> will ask resigned employee’s supervisor and then inform the <a href="#">Administration Department</a> of whether to delete the account or to redirect the e-mails to another account: -</p> <ul style="list-style-type: none"> <li>• If e-mails are to be redirected: The <a href="#">Administration Department</a> is to change the password of the e-mail to prevent unauthorized access.</li> <li>• For accounts to be deleted: The <a href="#">Administration Department</a> is to delete such email accounts from the Institute’s Web Server.</li> </ul>	<p><a href="#">Issuance and Exit Clearance Form</a> (HR Executive)</p>

<p>4.2 Note: As part of the Institute’s Confidentiality and Security of Information Process, staff that resigned will also need to complete the <a href="#">Issuance and Exit Clearance Form</a>.</p>	
<p><b>5. Access to Computerized Institute Management System</b></p> <p>5.1 The <a href="#">Administration Department</a> is to generate a <a href="#">Staff Access Rights Overview</a>. The overview is to be filled with the different access rights that staff are assigned to. If there are new positions or positions that have been removed, the <a href="#">Administration Department</a> will update the overview.</p> <p>5.2 The <a href="#">Management Team</a> is to approve this overview once a year.</p> <p>5.3 In the event that any staff has the need to access the Institute Management System, they are to put up an official request, through the <a href="#">Access Rights Request Form</a>, to the <a href="#">Administration Department</a>. The request should state the following: -</p> <ul style="list-style-type: none"> <li>• Staff Name</li> <li>• Staff Department</li> <li>• Staff Designation</li> <li>• Types / Levels of Access Rights</li> <li>• Reason / Purpose for Access Rights</li> </ul> <p>5.4 The staff will include whether the request for access is within his/her assigned rights, and seek <a href="#">Management</a> approval if the request is beyond those assigned.</p> <p>*Note: New staff going through orientation will also need to complete the form, to acknowledge the different access rights they have.</p> <p>5.5 The <a href="#">Administration Department</a> will edit the access rights upon approval. The staff and <a href="#">Administration Department staff</a> will sign on the <a href="#">Access Rights Request Form</a> as acknowledgement of the change.</p>	<p><a href="#">Staff Access Rights Overview</a> (<a href="#">Administration Department</a>)</p> <p><a href="#">Access Rights Request Form</a> (<a href="#">Administration Department</a>)</p>
<p><b>6. General Use of Computer, Network and Internet</b></p> <p>6.1 Staff usage of the Institute’s computers are to subject to the following: -</p> <ul style="list-style-type: none"> <li>• All campus computing resources (desktops, servers, network devices, etc.) may not be used to participate in any activity that adversely affects other users or poses a security threat either to the campus or to external entities.</li> <li>• The Institute may remove unauthorized software if found in the Institute computers.</li> </ul> <p>6.2 All internet use shall be for business related purposes. Utmost care should be exercised when downloading information and files from the Internet to safeguard against malicious codes and inappropriate material.</p>	
<p><b>7. Reporting of Loss / Thefts / Damage</b></p>	

<p>7.1 All users must promptly report the following to <b>Administration Department</b> within 24 hours through the use of the <b>Facility Complaint Record Book</b>: -</p> <ul style="list-style-type: none"> <li>• Any loss of, or severe damage to, their hardware</li> <li>• Serious information security vulnerabilities known to exist</li> <li>• Instances of suspected disclosure of sensitive information to an inappropriate party / person</li> <li>• Victims of virus attack</li> </ul> <p>7.2 Should the missing laptop or devices contain sensitive information, immediate action shall be taken by the user to minimize the impact of the loss or theft (E.g. cutting off the power to the computer)</p>	<p style="text-align: center;"><b>Facility Complaint Record Book (Administration Department)</b></p>
<p><b>8. Review of Process</b></p> <p>8.1 The <b>Independent Internal Process Auditor</b> will review the process as part of his/her Internal Process Review, Audit, and Assessment of the Institute.</p> <p>8.2 In addition, the Process Owner will do a review of the process at least once a year to ensure that it is up to date and relevant.</p>	<p style="text-align: center;"><b>IPRAA Report (Independent Internal Process Auditor)</b></p>

**FLOWCHART: CONFIDENTIALITY AND SECURITY OF INFORMATION**

