There are six ratings in film classification. They are:

- G - General
- PG - Parental Guidance
- PG13 - Parental Guidance for Children below 13
- NC16 - No Children below 16 years of age
- M18 - Mature 18, for persons 18 years and above
- R21 - Restricted to persons 21 years and above

G, PG and PG13 categories are advisory ratings while NC16

Information Classification

Information Classification Definitions

The following table provides a summary of the information classification levels that have been adopted by LSE and which underpin the 8 principles of information security defined in the Information Security Policy (Section 3.1). These classification levels explicitly incorporate the Data Protection Act's (DPA) definitions of *Personal Data* and *Sensitive Personal Data*, as laid out in LSE's Data Protection Policy, and are designed to cover both primary and secondary research data.

1. **Confidential**
   'Confidential' information has significant value for LSE, and unauthorized disclosure or dissemination could result in severe financial or reputational damage to LSE, including fines of up to £500,000 from the Information Commissioner's Office, the revocation of research contracts and the failure to win future research bids. Data that is defined by the Data Protection Act as *Sensitive Personal Data* falls into this category. Only those who need explicitly need access must be granted it, and only to the least degree in order to do their work (the 'need to know' and 'least privilege' principles). When held outside LSE, on mobile devices such as laptops, tablets or phones, or in transit, 'Confidential' information must be protected behind an explicit logon and by AES 256-bit encryption at the device, drive or file level.

logon and by AES 256-bit encryption at the device, drive or file level.

2. **Restricted**
'Restricted' information is subject to controls on access, such as only allowing valid logons from a small group of staff. 'Restricted' information must be held in such a manner that prevents unauthorised access i.e. on a system that requires a valid and appropriate user to log in before access is granted. Information defined as *Personal Data* by the Data Protection Act falls into this category. Disclosure or dissemination of this information is not intended, and may incur some negative publicity, but is unlikely to cause severe financial or reputational damage to LSE. Note that under the Data Protection Act large datasets (>1000 records) of 'Restricted' information may become classified as Confidential, thereby requiring a higher level of access control.

3. **Internal Use**
'Internal use' information can be disclosed or disseminated by its owner to appropriate members of LSE, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.

4. **Public**
'Public' information can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

MALAYSIAN PUBLIC SECTOR MANAGEMENT OF INFORMATION & COMMUNICATIONS TECHNOLOGY SECURITY HANDBOOK (MyMIS)

Version: 2

As of: 15 January 2002

Author: MAMPU

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Jawatankuasa Standard Keselamatan IT Kerajaan
Malaysian public sector management of information & communication technology security handbook / [Jawatankuasa Standard Keselamatan IT Kerajaan].
ISBN 983-9827-16-2
1. Computer security-Malaysia-Handbooks, manuals, etc.
2. Data protection-Malaysia-Handbooks, manuals, etc.
3. Administrative agencies-Data processing-Security measures-Malaysia-Handbooks, manuals, etc.
4. Administrative agencies-Communication systems-Security measures-Malaysia-Handbooks, manuals, etc.
5. Information technology-Security measures-Handbooks, manuals, etc. I. Title.
352.37909595

Chapter 3 BASIC OPERATIONS

This chapter discusses fundamental operational components

To implement effective Public Sector ICT Security will require strong commitment from the various level of organisations within the government. ICT security as a programme encompasses a wide spectrum of topics such as technology, people, finance, training, policy, risk management, processes and measures taken in total to safeguard the government's information and communications systems. This chapter explains some fundamental operational components of ICT security that should be imparted to public sector employees. Major areas include information classification, roles and responsibilities, human factors, electronic facilities, document management, storage management, contingencies, incident handling and physical and environmental protection.

3.1 Information Classification

4 classifications of official matters–Rahsia Besar, Rahsia, Sulit and Terhad

Official matters are graded into four classifications i.e. *Rahsia Besar, Rahsia, Sulit* and *Terhad* as stipulated in the *Arahan Keselamatan*.

Information content created digitally follow similar classification. However the protection of digital information requires different handling needs when compared to paper-based information such as encryption, colour coding, labelling, precaution against piggybacking and electronic eavesdropping e.g. tempest (Refer to Table 3.1 and Figure 3.1).

Mode	Conventional	Digital
Media	Hard copy	Digital Information
Handling	As per *Arahan Keselamatan*	Handling protection (As per Figure 3.1)

Table 3.1: Conventional vs. Digital Information Handling

3.2 Roles and Responsibilities

Management involvement is critical to ICT security. Capital expenditures alone cannot accomplish security. Management concern and effort are needed to plan, guide, motivate, and control an effective ICT security programme via the formation of ICT Security forum. A balanced programme, with proper concern for practicality and human values, will enhance the overall effectiveness of the information processing function.

3.2.1 Head of Department

Roles of Head of Department

Heads of Department are owners of Public Sector ICT assets and are accountable for their safe-keeping and protection. Essentially, the Head of Department should realise the importance of Public Sector ICT Security before it is implemented across the entire organisation. The Head of Department needs to be responsible for and supportive of ICT security programmes, promote compliance to standards, procedures and guidelines, and align Public Sector ICT Security requirements to the department's missions and objectives. In addition, the Head of Department should ensure adequate resources, both financial and personnel, are available for the programmes.

The roles and responsibilities of the Head of Department include:

(a) ensure all users including government employees, vendors and contractors understand the need for Public Sector ICT Security policy, standards and guidelines;

(b) ensure all users including government employees, vendors and contractors abide by the Public Sector ICT Security policy, standards and guidelines (necessary action must be taken upon non-compliance of any security measure);

(c) undertake evaluation of risk and security programmes based on the Public Sector ICT Security policy, standards and guidelines;

(d) develop an Adherence Compliance Plan for the purpose of managing risk arising from non-compliance of the Public Sector ICT Security policy, standards and guidelines; and

(e) report to MAMPU and other relevant authorities as required under *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) - Pekeliling Am Bil. 1/ 2001* dated 4 April 2001 the following:

3.1 Information Classification

4 classifications of official matters–Rahsia Besar, Rahsia, Sulit and Terhad

Official matters are graded into four classifications i.e. *Rahsia Besar, Rahsia, Sulit* and *Terhad* as stipulated in the *Arahan Keselamatan*.

Information content created digitally follow similar classification. However the protection of digital information requires different handling needs when compared to paper-based information such as encryption, colour coding, labelling, precaution against piggybacking and electronic eavesdropping e.g. tempest (Refer to Table 3.1 and Figure 3.1).

Mode	Conventional	Digital
Media	Hard copy	Digital Information
Handling	As per *Arahan Keselamatan*	Handling protection (As per Figure 3.1)

Table 3.1: Conventional vs. Digital Information Handling

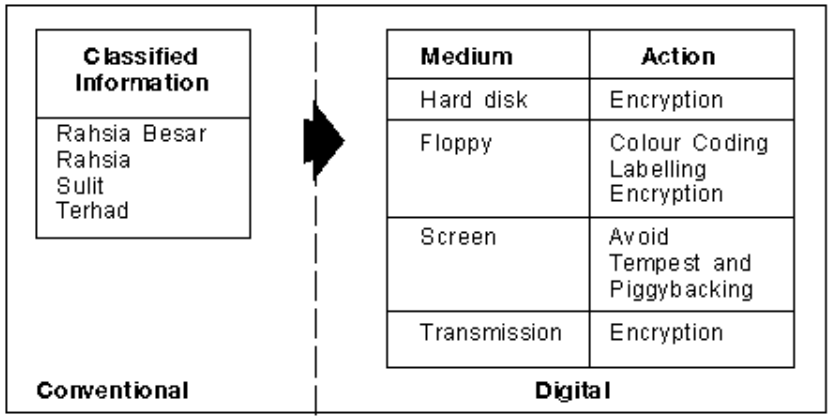

Figure 3.1: Handling Protection

	Confidential (highest, most sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
Description	Data which is legally regulated; and data that would provide access to confidential or restricted information.	Data which the Data Managers have not decided to publish or make public; and data protected by contractual obligations.	Data which there is no expectation for privacy or confidentiality.
Legal Requirements	Protection of data is required by law.	Protection of data is at the discretion of the **Data** Manager or **Data** Custodian.	Protection of data is at the discretion of the **Data** Manager or **Data** Custodian.
Reputation Risk	High	Medium	Low
Data Access and Control	Legal, ethical, or other constraints prevent access without specific authorization. Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements; and typically on a business "need to know" basis.	May be accessed by Clark employees and non-employees who have a business "need to know."	No access restrictions. Data is available for public access.
Transmission	Transmission of Confidential data through any non-Clark network or Clark guest network is prohibited (e.g. Internet). Transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is also prohibited.	Transmission of Restricted data through any wireless network, and any non-Clark wired network is strongly discouraged. Where necessary, use of the University's VPN is required. Transmission through any electronic messaging system (e-mail, instant messaging, text messaging), is also strongly discouraged.	No other protection is required for public information; however, care should always be taken to use all University information appropriately.
Storage	Storage of Confidential data is prohibited on unauthorized Qualified Machines and Computing Equipment unless approved by the Information Security Officer. If approved, ITS approved encryption is required on mobile Computing Equipment. ITS approved security measures are also required if the data is not stored on a Qualified Machine. Storage of credit card data on any Computing Equipment is prohibited.	Level of required protection of Restricted data is either pursuant to Clark policy or at the discretion of the Data Manager or Data Custodian of the information. If appropriate level of protection is not known, check with Information Security Officer before storing Restricted data unencrypted.	No other protection is required for public information; however, care should always be taken to use all University information appropriately.
Documented Backup & Recovery Procedures	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are not necessary, but strongly encouraged.	Documented backup and recovery procedures are not necessary, but strongly encouraged.
Documented Data	Documented data retention policy is required	Documented data retention policy is required	Documented data retention policy is not required,

Process + People + Technology

Adobe Reader - [http___pttgrpintranet.pttgrp.com_pttict_DocumentCenter_PTTICTCommand...

File Edit View Document Tools

Save a Copy Search

Pages Attachments Comments

ptt ICT

คำสั่ง บริษัท พีทีที ไอซีที โซลูชั่นส์ จำกัด

ที่ 62 /2553

เรื่อง นโยบายการจัดระดับชั้นความลับของข้อมูล

(Information Classification Policy)

.....

เนื่องจากข้อมูลมีความสำคัญต่อการดำเนินธุรกิจ จึงจำเป็นต้องมีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมตามลำดับชั้น ทั้งนี้เพื่อให้มีการบริหารจัดการอย่างเหมาะสม มีประสิทธิภาพ และเป็นไปตามแนวปฏิบัติสากล บริษัทจึงขอประกาศนโยบายการจัดระดับชั้นความลับของข้อมูล โดยมีสาระดังต่อไปนี้

8.51 x 11.65 in

1 of 2

start 5 Micros... STAFF MTG 2 Micros... http___ptt... http___ptt... EN 9:02 AM

Information_classification_policy.pdf - Adobe Reader

Edit View Document Tools Window Help

1 / 2 133% Find

คำสั่งบริษัท ปตท. จำกัด (มหาชน)

ที่ 05 /2554

เรื่อง นโยบายการจัดระดับชั้นความลับของข้อมูล

(Information Classification Policy)

สถาบันวิจัยและเทคโนโลยี ปตท.

เนื่องจากข้อมูลวิจัยมีความสำคัญต่อการดำเนินงานวิจัยและพัฒนา จึงจำเป็นต้องมีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมและให้มีการบริหารจัดการอย่าง มีประสิทธิภาพและเป็นไปตามแนวปฏิบัติสากล จึงขอประกาศนโยบายการจัดระดับชั้นความลับของข้อมูล โดยมีสาระสำคัญ ดังต่อไปนี้

ข้อ 1 ข้อมูลที่มีความสำคัญต่อการดำเนินงานวิจัยและพัฒนาของสถาบันวิจัยและเทคโนโลยี ปตท. จึงต้องได้รับการกำหนดระดับชั้น

EN 13:22 27/6/2011

PTT RTI Information Classification

Classification	Public (ข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้)	PTT Group Internal use only (ข้อมูลที่ใช้ภายในบริษัท ปตท. และกลุ่มบริษัท ปตท.เท่านั้น)	PTT RTI Internal use only (ข้อมูลที่ใช้ภายในสถาบันวิจัยและเทคโนโลยี ปตท.เท่านั้น)	Confidential (ข้อมูลลับ)	Top Secret (ข้อมูลลับที่สุด)
Sensitivity Level	Open or unclassified	Low	Moderate	High	Critical
Definition	**Public information** is information that can be disclosed to anyone without violating an individual's right to privacy. Knowledge of this information does not expose the corporation to financial loss, embarrassment, or jeopardize the security of assets.	**PTT Internal use only information** is information that, due to technical or business sensitivity, is limited to employees and contractor who work outside PTT RTI and in the PTT Group. It is intended for use only within the corporation. Unauthorized disclosure, compromise, or destruction would not have a significant impact on the corporation or its employees.	**PTT RTI Internal use only information** is information that, due to technical or business sensitivity, is limited to employees and contractor who work on-site PTT RTI. It is intended for use only within the corporation. Unauthorized disclosure, compromise, or destruction would not have a significant impact on the corporation or its employees.	**Confidential information** is information that the corporation and its employees have a legal, regulatory, or social obligation to protect. It is intended for use solely within defined groups in the corporation. Unauthorized disclosure, compromise, or destruction would adversely impact the corporation or its employees.	**Top secret information** is the highest level of classification, information whose unauthorized disclosure, compromise, or destruction could result in severe damage, provide significant advantage to a competitor, or incur serious financial impact to the corporation or its employees. It is intended solely for restricted use within the corporation and is limited to those with an explicit, predetermined "need to know."
Level of security	• File convention to .pdf only	• Passwords • Encryption keys	• Passwords • Encryption keys	• Passwords • Encryption keys	• Passwords • Encryption keys

Announced on Jun 01, 2011

6/28/2011

PTT RTI Information Classification Practices

Classification	Public (ข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้)	PTT Group Internal use only (ข้อมูลที่ใช้ภายในบริษัท ปตท. และกลุ่มบริษัท ปตท.เท่านั้น)	PTT RTI Internal use only (ข้อมูลที่ใช้ภายในสถาบันวิจัยและเทคโนโลยี ปตท.เท่านั้น)	Confidential (ข้อมูลลับ)	Top Secret (ข้อมูลลับที่สุด)
Level of security	• File convention to .pdf only	• Passwords • Encryption keys	• Passwords • Encryption keys	• Passwords • Encryption keys	• Passwords • Encryption keys
Right of accessibilities	Public	Employee and PTT RTI VP in PTT Group	Employee and PTT RTI VP in each department	PTT RTI VP	PTT RTI EVP/ Selected PTT RTI VP
Right of accessibility Approved by	PTT RTI VP/ PTT RTI EVP	PTT RTI VP/ PTT RTI EVP	PTT RTI VP/ PTT RTI EVP	PTT RTI VP/ PTT RTI EVP	PTT RTI VP/ PTT RTI EVP
Right of accessibility announced by	PTT RTI EVP	PTT RTI EVP	PTT RTI EVP	PTT RTI EVP	PTT RTI EVP
Information Inventory	- RTI Profile and RTI Capabilities - ข้อมูลสำหรับสื่อต่าง ๆ - ข้อมูลตอบแบบสอบถามจากหน่วยงานภายนอก ปตท. -รายงานประจำปีของ ปตท. ตามแบบ 56-1(R&D Section) -รายงานประจำปีของ ปตท. ตามแบบ 69-1(R&D Section) -PTT Annual Report (R&D Section) -รายงานผลการดำเนินงานโครงการพัฒนาพลังงานหมุนเวียน ตามยุทธศาสตร์แผนพัฒนาเศรษฐกิจและสังคมฯ น้าส่งกระทรวงพลังงาน - PTT RTI Newsletter - etc.	- ข้อมูลตอบแบบสอบถามจาก หน่วยงานภายใน ปตท. - รายงานการขอปรับงบประมาณกลางปีพร้อมเหตุผลการปรับงบประมาณ - การขอผูกพันงบประมาณและแผนงาน Work Program ประจำปี - แผนจัดซื้อจัดจ้างประจำปี - แผนจัดซื้อจัดจ้างครุภัณฑ์ราคาเกิน 2 ล้านบาท ที่ดิน สิ่งก่อสร้างที่มีราคาเกิน 15 ล้านบาท - กรอบอัตรากำลังและ scope งานพนักงานและ contract 5 ปี - Minute PTT R&T Group Committee - รายงานความคืบหน้า PA/KPI - etc.	- PTT RTI Roadmap and Positioning of each department - PTT RTI STS Y..... - Minute PTT RTI MC - Minute PTT RTI Project - RTI Weekly News - รายงานการประชุมประจำเดือนของหน่วยงาน - Report, Presentation File ที่ใช้เฉพาะใน สวญ. - Work Instruction - Environmental Sharing Database - Software Program (limited user) - Budget Planning and Reporting - etc.	- WP/IO Monthly Progress Report - 5-Year RTI BU Plan - รายงานผลการปฏิบัติงานประจำเดือน - Data and Information of Research Project - Data and Information of Commercial Test /Licensing/Implementation Application - Data and Information of Original Equipment Manufacturer Approval - Data and Information of Third Party Certified - PTT RTI Testing Service for Customer within PTT Group - etc.	- Product Formula - Recipe - In-house Procedure - Know-how - Lab Book - ข้อมูลที่เกี่ยวข้องในเชิงวิจัยและธุรกิจ เช่น M&A deals - Product Drawing - Product Prototype - Designated Top Secret Research Report or Document - etc.