



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy Compliance Assessment Report

On

Smart Identity Card System
(SMARTICS)

July 2010

This page is intentionally left blank to facilitate double-side printing

Table of Contents

1. Introduction	1
<i>Background</i>	1
<i>Memorandum of Understanding signed between PCPD and the ImmD</i>	4
2. Privacy Compliance Assessment	6
<i>Purpose</i>	6
<i>Scope</i>	6
<i>Limitations</i>	6
<i>Privacy Impact Assessment</i>	7
<i>Methodology</i>	8
<i>Duration of the PCA</i>	12
3. Smart ID Card Data	13
<i>Smart ID Card Application</i>	13
<i>Access of Smart ID Card Data</i>	15
<i>Third Party Service Providers</i>	16
4. Policy Review	17
<i>Policy Review</i>	17
<i>Governance</i>	18
<i>DPP1 – Purpose and Manner of Collection of Personal Data</i>	25
<i>DPP2 – Accuracy and Duration of Retention of Personal Data</i>	28
<i>DPP3 – Use of Personal Data</i>	30
<i>DPP4 – Security of Personal Data</i>	33
<i>DPP5 – Information to be Generally Available</i>	42
<i>DPP6 – Access to Personal Data</i>	43
5. Workflow Review	47
<i>Workflow Review</i>	47
<i>Governance</i>	48
<i>DPP1 – Purpose and Manner of Collection of Personal Data</i>	56
<i>DPP2 – Accuracy and Duration of Retention of Personal Data</i>	57
<i>DPP3 – Use of Personal Data</i>	62
<i>DPP4 – Security of Personal Data</i>	63
<i>DPP5 – Information to be Generally Available</i>	78
<i>DPP6 – Access to Personal Data</i>	79
6. Conclusion	81
Glossary	83
Appendix I – Personal Data (Privacy) Ordinance	85

Appendix II – Documents reviewed during Policy Review.....	90
Appendix III – Offices visited.....	102
Appendix IV – Questionnaire for identity card applicants.....	103
Appendix V – Questionnaire for staff of Immigration Department.....	110
Appendix VI – Photographs taken at Immigration Department.....	132

Introduction

Background

- 1.1 Under the Registration of Persons Ordinance, Cap. 177 (“**ROP Ordinance**”), every person in Hong Kong is required to be registered in such manner as shall be prescribed in the regulations made under the ROP Ordinance. In accordance with the Registration of Persons Regulations, Cap. 177A (“**ROP Regulations**”), every person who is not an exempt person (e.g. children under 11 years of age) or an excluded person is required to register for an identity card within 30 days of his/her entering Hong Kong. In the case that this person is already in Hong Kong when he/she becomes required by the ROP Ordinance or related regulations to be registered, this person shall within 30 days of the date when he/she is so required, whichever is the sooner, to apply for an identity card.
- 1.2 The Government of the Hong Kong Special Administrative Region (the “**Government**”) introduced a new Hong Kong identity card in the form of a smart card (“**Smart ID Card**”). The Registration of Persons (Amendment) Bill 2001 (“**Bill**”) was tabled before the Legislative Council (“**LegCo**”) in January 2001. It aimed to provide the legislative framework for the Smart ID Card with multi-application capacity. To provide for the “smart element” of the Smart ID Card, i.e. an integrated circuit (“**Chip**”) and the data stored in it, the Bill proposed to amend Schedule 1 to the ROP Regulations to specify the kind of data that were to be stored in the Smart ID Card. After scrutiny by a Bills Committee, the Bill was passed with amendments by LegCo on 19 March 2003.
- 1.3 Upon passing of the Bill and for the purpose of introducing the Smart ID Card, a new supporting information system, known as the Smart Identity Card System (“**SMARTICS**”) was launched by the Immigration Department (“**ImmD**”) which would be used to store all the identity card related information. SMARTICS was

designed to support the processing, personalization and issuing of Smart ID Cards and the related record management function. The exercise to replace the existing identity cards held by holders by the issuance of the Smart ID Cards was carried out in phases and was completed on 31 March 2007. As at 31 December 2009, a total of 8,868,356 Smart ID Cards were issued.

1.4 The following personal data (“**Smart ID Card Data**”) set out in Schedule 1 to the amended ROP Regulations are stored/processed by the ImmD’s SMARTICS, and stored in the new Smart ID Cards:

- (a) the full personal name and surname of the applicant in English or in English and Chinese;
- (b) the Chinese commercial code (if applicable);
- (c) the date of birth of the applicant;
- (d) a number for identification purpose;
- (e) the date of issue of the card;
- (f) a photograph of the applicant, unless the applicant is under the age of 11 years;
- (g) such data, symbols, letters or numbers representing prescribed information, particulars or data within the meaning of section 7(2A)(b) of the ROP Ordinance as the Director of Immigration may determine; and
- (h) template of the applicant’s thumb-prints or other fingerprints taken under the ROP Regulations; and
- (i) (where the applicant does not have a right of abode in Hong Kong) the conditions of stay (including a limit of stay) imposed in relation to him under section 11 of the Immigration Ordinance (Cap. 115).

1.5 The Smart ID Card is also designed to enable the use of the Smart ID Card Data for non-immigration purposes as lawfully permitted. Currently, the Leisure and Cultural Services Department (“**LCSD**”) is the sole authorized party who can access the card face compartment for non-immigration use. The data in the card face compartment includes identity card number, English name, Chinese name (unicode), date of birth and date of registration.

With the consent of Smart ID Card holders, library staff may collect the data in the card face compartment and transfer them to LCSD's computer system for the purpose of library card registration.

- 1.6 Additionally, Smart ID Card holders may opt-in to embed the Hongkong Post digital certificate (the “**e-Cert**”) into the Chips of their Smart ID Cards. Subscribers, who had been issued with passcodes for the e-Cert, will then need smart card readers and associated software to use the e-Cert for certain online government services or other commercial operations requiring online digital signature or authentication.
- 1.7 The compliance of SMARTICS in collecting, processing and handling Smart ID Card Data with the requirements of the Personal Data (Privacy) Ordinance (Cap. 486) (the “**Ordinance**”) is therefore of great public concerns in view of:
 - (i) the statutory obligation of every person in Hong Kong to register for an identity card under the ROP Ordinance;
 - (ii) almost every individual in Hong Kong is being affected;
 - (iii) the unique and normally unchangeable nature of the data, for instance, ID number, date of birth, fingerprint template being collected and processed;
 - (iv) the vast and important database held by ImmD which will be built up and amassed over time; and
 - (v) the grave and adverse privacy consequences that could cause data subjects if their personal data are improperly handled or if there is any data breach.
- 1.8 The ImmD was therefore committed to seek assistance from the Office of the Privacy Commissioner for Personal Data (“**PCPD**”) to conduct a Privacy Compliance Assessment (“**PCA**”) of the personal data system with respect to Smart ID Card Data on its compliance with the Ordinance.
- 1.9 In view of the great public interest in ensuring that the Smart ID Card Data are collected and processed in compliance with the requirements of the Ordinance, the Privacy Commissioner for

Personal Data (the “**Commissioner**”) had decided to undertake a PCA for SMARTICS.

- 1.10 The conducting of the PCA was consistent with the Commissioner’s regulatory function under section 8(1)(c) of the Ordinance to promote awareness and understanding of, and compliance with, the provisions of the Ordinance, in particular, the data protection principles (“**DPPs**”).

Memorandum of Understanding signed between PCPD and the ImmD

- 1.11 With the objective of promoting and monitoring compliance with the requirements of the Ordinance, the Commissioner entered into a Memorandum of Understanding (“**MoU**”) with the Director of Immigration on 5 June 2009 to evaluate whether the ImmD had taken effective measures to comply with the requirements of the Ordinance including the DPPs in relation to the Smart ID Card Data. The results of the PCA would be considered by the ImmD in revising and fine-tuning the “Draft Code of Practice on Smart Identity Card Data” (“**Draft Code of Practice**”) to be submitted to the Commissioner for approval under section 12(1) of the Ordinance.
- 1.12 According to the MoU, the procedures of the operation of the SMARTICS would be walked through during the PCA with the purpose of assessing the level of compliance with the Ordinance by the Commissioner, identifying potential weaknesses in the personal data system in relation to the Smart ID Card Data and providing information and recommendations to ImmD for review.
- 1.13 Since the Draft Code of Practice had not been formally issued within the ImmD for compliance, it was not used as a benchmark during the assessment but only as a reference material to understand the controls in place.

- 1.14 The Director of Immigration undertook to revise and fine-tune the Draft Code of Practice based on the results and recommendations of the PCA. The final version of the Code of Practice will then be submitted for the formal approval by the Commissioner. The Code of Practice¹ (“**Code of Practice**”), as approved, shall then provide the practice for ImmD, its authorized staff and agents for the purpose of protecting personal data and as a benchmark for any subsequent PCAs.
- 1.15 The MoU expressly excluded the assessment on the compliance with the Ordinance by other parties or other government departments who might have access to all or part of the Smart ID Card Data, whether printed on the face of or stored in the Chip embedded in a Smart ID Card.
- 1.16 It is expressly acknowledged in the MoU that the conduct of the PCA was without prejudice to the statutory functions and powers vested in the Director of Immigration and the Commissioner.
- 1.17 Having completed the PCA in accordance with the terms of reference of the MoU, the Commissioner presents to the Director of Immigration this Report (“**Report**”) with its observations, findings, recommendations and conclusion.

¹ The provisions of the Code of Practice are not legally binding. A breach of the Code of Practice by ImmD, however, will give rise to certain presumptions against ImmD. Basically the Ordinance provides that:

- (a) where a Code of Practice has been approved by the Commissioner in respect of any requirements of the Ordinance;
- (b) if it is necessary to prove any matter in order to establish contravention of a requirement under the Ordinance in any proceedings under the Ordinance;
- (c) that matter shall be taken as proved if it is proved that there was at any material time failure to observe any provision of the Code of Practice relevant to that matter.

unless there is evidence that the requirement of the Ordinance was actually complied with in a different way, notwithstanding the non-observance of the Code of Practice.

Privacy Compliance Assessment

Purpose

- 2.1 The PCA aimed at assessing and evaluating the level of privacy compliance with the Ordinance, in particular the six DPPs² in Schedule 1 to the Ordinance, by the ImmD with respect to the collection, processing and handling of the Smart ID Card Data.

Scope

- 2.2 The main scope of the PCA includes:
- ◆ the assessment of ImmD’s level of compliance with the requirements of the Ordinance, in particular the six DPPs;
 - ◆ the identification of the potential weaknesses in ImmD’s personal data system for handling Smart ID Card Data; and
 - ◆ the making of observations and recommendations for review by ImmD of its personal data system for handling Smart ID Card Data.

Limitations

- 2.3 The PCA was conducted on a consensual basis since it was neither an inspection nor an investigation carried out under the Ordinance. In conducting the PCA, PCPD relied on the information and documents that were made available to it and the facilities offered by the ImmD.
- 2.4 Since the Ordinance is technology-neutral, the PCA did not assess the technical IT aspects of SMARTICS but focused on the evaluation of management controls from an administrative perspective. For instance, focus was not put on the stringency of encryption algorithm but on the fulfilment of the Government’s requirements for employing encryption technology to achieve

² The six DPPs are listed in **Appendix I**. Detailed explanation and expectation on how to fulfil them are listed under Chapter 4 and Chapter 5.

personal data protection.

- 2.5 Other potential non-immigration use of the Smart ID Card Data and their corresponding data protection procedures at the Smart ID Card Chip were out of the purview of this assessment. According to the Government's response provided to the LegCo, such potential use would not be implemented without the approval of the LegCo.
- 2.6 For the purpose of conducting the PCA, ImmD was considered as the sole data user. The PCA was not concerned with the existing non-immigration use nor the data protection practices of other parties which might receive the Smart ID Card Data directly or indirectly from ImmD. The acts and practices of other government departments and other parties who have access to all or some parts of the Smart ID Card Data were likewise out of the scope of this PCA.
- 2.7 By the same token, the PCA was confined to reviewing ImmD's control measures imposed upon its third party service providers. The PCA did not assess or examine the system run and adopted by third party service providers.
- 2.8 The findings in this Report represent a reflection of the controls in place during the period of observation. Nevertheless, reasonable inference had been drawn from those findings for projecting a bigger picture of the state of personal data security in SMARTICS.
- 2.9 In view of the circumstances mentioned above, the findings and recommendations made in this Report shall not be treated as exhaustive to cover every aspect of the SMARTICS operation on a continuous basis but shall only be regarded as verifications of the compliance level of the matters in question at the time when the assessment and observations were made.

Privacy Impact Assessment

- 2.10 During the very early stage of the SMARTICS project, PCPD

expressed its concern on the necessary privacy protection and stressed the importance of the Privacy by Design³ principle. The Commissioner at the time highlighted to the Deputy Director of Immigration the need for a Privacy Impact Assessment (“**PIA**”) to be conducted to identify areas where special privacy attentions would be needed.

2.11 ImmD took the advice and, from 2000 to 2005, employed independent consultants to conduct four PIAs. The identified issues were broadly discussed in LegCo in February 2001, July 2002, January 2004 and February 2005 respectively (see **Appendix II**).

2.12 A number of recommendations were made by the consultants in their PIA reports. ImmD also provided its responses in the formal discussions in the LegCo sessions. These reports and responses were noted and examined as part of the PCA. Chapter 4 of this Report examines whether all the recommendations had been addressed by ImmD.

Methodology

2.13 This section briefly describes the process of how the PCA was conducted.

2.14 It is worth noting that the Ordinance does not prescribe or define how a PCA should be conducted. In performance of his function to monitor and supervise compliance of the Ordinance and in view of the nature of SMARTICS, the Commissioner found it appropriate to conduct the PCA through policy/guideline/procedure review (“**Policy Review**”) and workflow review (“**Workflow Review**”). The bulk of the PCA work was on the Policy and the Workflow Reviews. More details can be found in Chapter 4 and Chapter 5 of this Report.

³ Privacy by Design is a principle whereby privacy compliance is designed into systems holding information right from the start and not as an after-thought. More explanation is given under Chapter 4.

- 2.15 This methodology adopted was not necessarily a standard approach to be followed by similar assessments in the future. Instead the Commissioner expects the methodology to evolve and change according to the specific subject matter to be assessed and other relevant circumstances.

Preliminary Preparation

- 2.16 The Commissioner assembled and led an Assessment Team (the “**Team**”) comprising PCPD officers to conduct the PCA. The Team started work by convening an initial meeting with ImmD on 26 June 2009 to discuss on the assessment approach and assistance required. The Team made detailed enquiries into the operation of SMARTICS and the use of Smart ID Card Data in terms of by whom and under what circumstances access would be allowed.

The Assessment

- 2.17 The PCA consisted of two major components: the Policy Review and the Workflow Review.

The Policy Review

- 2.18 The objective of the Policy Review was to ensure that there were sufficient and appropriate formal policies, guidelines and procedures in place. It was intended to be a test of adequacy in terms of these documentations. These documentations should have laid down the appropriate level and expectation of standards and protections to be followed by all who need to handle or have access to some or all of the Smart ID Card Data.

Documents Inspected

- 2.19 In order to assess whether ImmD had a documented privacy protection system and all the necessary policies and guidelines to comply with the requirements of the Ordinance, the Team examined thousands of pages of ImmD documents including policies, guidelines, internal circulars, memos, information

security incident procedures, operation manual procedures and training materials, as well as the summary of recommendations of the PIAs. A full list of documents examined can be found in **Appendix II**.

Workflow Review

- 2.20 The objective of the Workflow Review was to examine and assess whether all the formal policies, guidelines and procedures mentioned under the Policy Review were being complied with. The Workflow Review might be seen as a test of compliance in terms of whether policies, guidelines and procedures were being followed in practice. One key criterion was to look for sufficient evidence, either from documents or actual practice to assess the level of compliance.
- 2.21 Given the essence of the Workflow Review was to assess the level of compliance, the Team visited 19 offices and control points of ImmD (**Appendix III**) during the course of the Workflow Review to gather evidence and to interview staff and Smart ID Card applicants.

Interviews and Site Visits

- 2.22 The Team interviewed 65 ImmD officers ranking from Immigration Assistants to Assistant Directors between 24 September and 15 October 2009 located in the 19 ImmD offices and control points mentioned above.
- 2.23 ImmD facilities examined included public waiting areas at Registration of Persons Offices (“**ROP Office**”), service booths, processing areas, identity card production facilities, records-storage and destruction facilities, self-service kiosks, SMARTICS terminals, IT server rooms and data backup facilities. The handling, storage and physical security of the Smart ID Card Data were specifically examined during these site visits. The sites visited were specifically chosen after full discussions with ImmD in light of the importance of their heavy or specific interaction

with Smart ID Card Data.

Survey and Questionnaire

- 2.24 A survey was conducted face-to-face with 333 Smart ID Card applicants between 12 and 18 August 2009 (**Appendix IV**). The survey aimed to assess from the applicants' perspective whether the data protection measures taken by ImmD in the handling of Smart ID Card Data by staff in daily work were effective. 300 questionnaires (**Appendix V**) were also handed out to ImmD staff on 4 November 2009. The questionnaires were designed to examine the level of understanding and compliance of personal data protection from the perspective of the ImmD staff.
- 2.25 Results of the survey and questionnaires are helpful tools to give the Commissioner a glimpse of how data protection measures were implemented in daily operation and the level of awareness of ImmD staff on data protection, but they were not the only materials based upon which the Commissioner made his findings. These results must be read with caution because the size of the samples has been restricted by the limited resources of the PCPD, the varying degrees of involvements with Smart ID Card Data based on the respondents' duties and responsibilities, and the results only provide a snapshot of responses at a given time. Moreover, to avoid any possible distortion, isolated responses did not form any basis of the Commissioner's findings.

Discussions

- 2.26 Throughout the entire PCA exercise, the Team was in constant contact with the staff members of the ROP Division of ImmD who acted as the coordinator to provide documentation, explain and clarify issues, and facilitated access to all the information as requested by the Team.

Draft Recommendations and Response

- 2.27 After both the Policy and the Workflow Reviews had been completed, the Team consolidated all the findings and sought

clarifications, where necessary, before forming opinions and conclusions on specific issues. A draft report was then drawn up and passed to ImmD for its responses. Having considered ImmD's responses, this Report was finalised.

Closing Meeting

2.28 Before this Report was issued, the Commissioner convened a closing meeting with the Director of Immigration to discuss the findings and recommendations for follow-up actions to be taken.

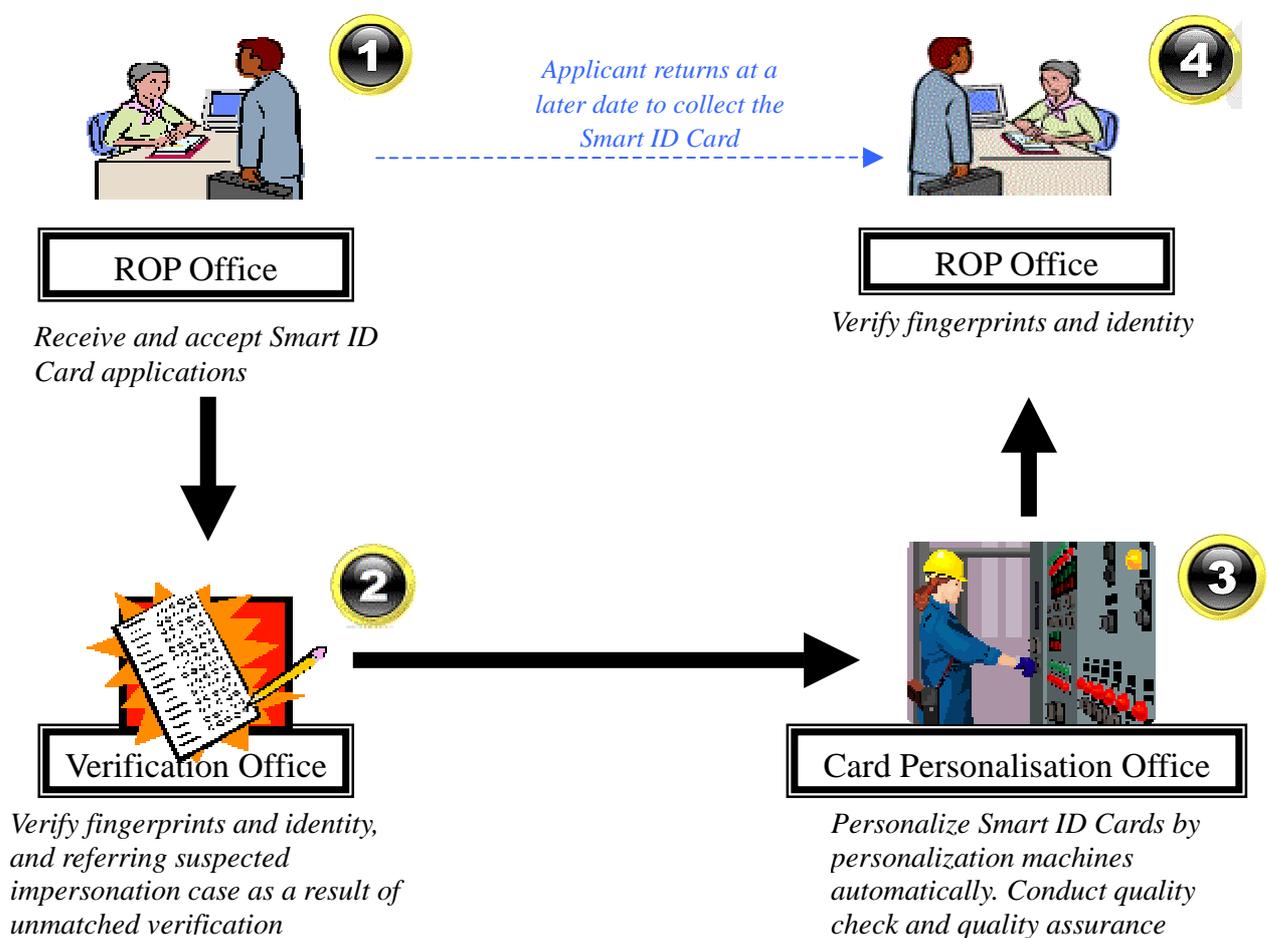
Duration of the PCA

2.29 The Team conducted the PCA during the period from July to November 2009, and prepared the draft report from November 2009 to March 2010.

Smart ID Card Data

Smart ID Card Application

3.1 The procedures for applying and processing an application for a Smart ID Card, at the time of the PCA, are illustrated in the diagrams below:



Smart ID Card Application Procedures

3.2 Applications for the Smart ID Cards are made through the ROP Office.

ROP Office

- 3.3 In the ROP Office, an Assistant Clerical Officer (“**ACO**”) will interview Smart ID Card applicants and capture the applicant’s facial and fingerprint images. Completed application forms and relevant supporting documents are then checked and scanned into SMARTICS by the ACO. The applications will then be assessed by an Immigration Officer (“**IO**”) to ascertain the identities, the guardianships (where applicable) and data accuracy in the applications. The IO will also verify the applicants’ live fingerprints against the images captured by the ACO to ensure accuracy and likeliness.
- 3.4 After these checks, the IO will approve the applications and the Smart ID Card Data collected will be forwarded to the Verification Office. The applicant will then be asked to return to the same ROP Office (the “**Originating ROP Office**”) to collect the Smart ID Card at a later date.

Verification Office

- 3.5 At the Verification Office, the accepted Smart ID Card applications will have the captured fingerprints verified by automatic matching against the applicants’ previous ROP records. A high or a low score will be generated from the automatic fingerprint matching. Every low score matching case will be scrutinized by manual comparison of the fingerprints on record or further examination on photographs or other documents held. The Verification Office needs to be satisfied with the identities before the Smart ID Card applications are moved to the next stage of card personalization.

Card Personalisation Office

- 3.6 The Card Personalisation Office is responsible for customising the personalized Smart ID Cards for verified applications received from the Verification Office. The personalisation process includes printing information on the card face and storing Smart ID Card

Data regarding an individual in the Chip of his/her Smart ID Card. The personalized Smart ID Cards will then undergo a quality assurance process. During the quality assurance process, batches of Smart ID Cards are tracked as they moved from one staff member to another. Afterwards, the personalized Smart ID Cards will be dispatched to the Originating ROP Office in a secured manner for collection.

Originating ROP Office

- 3.7 When an individual arrives to collect the Smart ID Card in the Originating ROP Office, ACO will ascertain the identity of the applicant or his/her authorized representatives before issuing the personalized Smart ID Card to him/her. If the applicant collects his/her Smart ID Card in person, the applicant will be required to match fingerprints against the Smart ID Card using fingerprint readers (Picture 1 in **Appendix VI**) installed in the ROP Offices.

Access of Smart ID Card Data

Immigration Use

- 3.8 Apart from the Smart ID Card application and verification process, information printed on the card face and stored in the Chip of Smart ID Card would be accessed by ImmD or the card holder for various purposes. The check points at various Immigration Control Points, such as cross border locations and the international airport, where such Smart ID Card Data are accessed by ImmD staff or e-Channel machines for immigration control is probably one of the most obvious purposes of access. Card holders may also access their Smart ID Card Data through self-service kiosks located at ROP Offices, Immigration Headquarters in Wan Chai and Immigration Control Points to verify the data held in the Chip of their Smart ID Cards by inserting the same into the readers in these kiosks.
- 3.9 Not only can information be directly accessed from card faces and Chips of Smart ID Cards, Smart ID Card Data can also be

retrieved from the information system for SMARTICS located in ImmD. One such unit within the ImmD that has access to Smart ID Card Data on a regular basis was the Confidential Records Unit (“CRU”). CRU handles Smart ID Card Data queries and requests from other government departments in accordance with section 11 of the ROP Ordinance.

Non-Immigration Use

- 3.10 As mentioned in paragraphs 1.5 and 1.6 in Chapter 1, the card face compartment data of the Smart ID Card Data could be used for the purpose of library card with consent from the card holders. Also, Smart ID Card holders can opt-in to embed the e-Cert into the Chips of their Smart ID Cards. These data may then be accessed by the relevant data users for the said purposes.

Third Party Service Providers

- 3.11 The work comprising the design, building and maintenance of the SMARTICS project was outsourced to an international consortium⁴ led by PCCW Business e-Solutions Limited as approved by the Central Tender Board of the Government.
- 3.12 Although the SMARTICS project has been outsourced to this consortium, no one in the consortium has direct access to Smart ID Card Data. The consortium’s employees have to be escorted and accompanied by an ImmD staff when they access the information system of SMARTICS for maintenance purpose.

⁴ Comprised of local companies such as SecureNet Asia Limited as well as international companies including Trüb from Switzerland, Cogent System Inc. from USA, Keycorp Limited from Australia, ACI Worldwide from Singapore and Mondex International from UK.

Policy Review

Policy Review

- 4.1 The objective of the Policy Review was to assess whether there were sufficient formal policies, guidelines and procedures in place. These documentations should have laid down the appropriate level and expectation of standards and protections to be followed by all who need to handle or had access to the relevant Smart ID Card Data.
- 4.2 Policies, guidelines and procedures are generally formulated in a hierarchical manner with a top-down approach. Management should set the overall but clear directions on the handling of personal data at the policy level. Such directions are then elaborated at the guidelines level to clarify expectations on behaviours and outcomes. In areas where further clarity or a higher degree of conformity is expected, procedures may be developed to ensure full compliance with the policies and guidelines.
- 4.3 It is understandable that there may not be a dedicated set of formal documentation devoted solely to personal data or privacy. However, it is expected that personal data or privacy handling are addressed in some formal documentations such as general policy, operating/office manuals, general security or IT security documents.
- 4.4 It is worth noting that while almost universally personal data of any size are kept in some form of information systems, the protection of personal data does not rest solely on the security of those information systems. Protection of personal data must be viewed end-to-end from collection to erasure/disposal. The scope of this Policy Review for SMARTICS, therefore, also included all matters such as processes, practices, human interactions and perceptions.

- 4.5 The following paragraphs attempt to systematically outline the controls to be examined for the protection of personal data. The controls listed below are by no means exhaustive or are universally accepted assessment standards. They merely serve as a convenient way of presenting the controls in a hierarchal manner. Since the handling of personal data is a complex topic and needs to be looked at holistically, certain areas may in fact interweave across multiple topics in practice. Additionally, the controls listed below need to evolve in accordance with the expectation of the public as personal data protection develops.

Governance

- 4.6 Governance forms the backbone of personal data protection as it provides a formal and sustainable framework of controls. Privacy protection governance may include, but is not limited to the following controls:

4.6.1 Structured Management Control

The roles and responsibilities of all relevant SMARTICS stakeholders from ImmD management, officers to technology professional people should be clearly defined, documented and promulgated. Supervision and monitoring should be an integral part of the roles and responsibilities of these stakeholders.

4.6.2 Privacy by Design

Privacy by Design is a principle according to which privacy compliance is designed into the systems holding information right from the start and not as an after-thought. The emphasis of the Privacy by Design principle is about proactive planning, preventive measures and end-to-end consideration. One key starting point of the Privacy by Design principle is to conduct PIA at the early stage of any project/initiative

involving personal data so that any findings and recommendations will be visible and given prominent attention throughout the project/initiative.

4.6.3 **Documentation**

Appropriate policies, guidelines and procedures addressing personal data protection should be formally available to facilitate compliance and consistency in approach. There should be a “lifecycle” management system for those formal documents including approval, promulgation, regular reviews, version-control, dissemination to stakeholders and updating or deletion.

4.6.4 **Data Classification**

Data classification helps to determine and highlight the level of sensitivity of different Smart ID Card Data. It helps to facilitate the application of the “need-to-know” or “least-privileged access” principles in the protection of personal data stored. It also allows appropriate controls to be applied to different classes of Smart ID Card Data thus channelling resources and attentions to the corresponding level of protection for those personal data.

4.6.5 **Assessment/Audit**

Assessment or audit closes the loopholes by examining the compliance and effectiveness of all the standards and controls, whether to be followed by the stakeholders or applied to any processes or practices, against the applicable laws, regulations, policies and practices. A formal and regular programme of assessment or audit of the right depth will help to identify gaps and plan for improvements.

4.6.6 **Data Breach Management**

Data breach management is important for organizations which process personal data. It usually consists of containment of situation, recovery planning, risk assessments and notification of breaches. An effective data breach management system can facilitate organizations to take appropriate measures to stop or prevent the recurrence of data breaches and mitigate accidental loss, destruction of or damage to personal data.

4.6.7 **Training and Awareness**

Training and awareness are the key means to realize all the expectations and controls. There should be a formal programme to ensure that proper and up-to-date training is provided to all internal stakeholders. The level of awareness needs to be assessed continuously to ensure the effectiveness of the training programme.

General Comments

4.7 In carrying out the Policy Review, the Team examined a large number of documents which are listed in **Appendix II**. Documents regarding policies, guidelines, manuals, procedures, reports, memoranda, circulars and plans for SMARTICS, workflows/processes, user sections, incident handling and devices were provided by ImmD. These documents were examined by the Team to assess whether all the six DPPs are properly addressed.

4.8 After examining and cross-referencing all the documentations provided by ImmD, the Commissioner was generally satisfied that the supplied documentations do cover the general control of Governance, with the exceptions mentioned under the “Specific Findings” below.

4.9 ImmD followed the Privacy by Design principle and

commissioned PIAs to be carried out throughout the SMARTICS project. ImmD then made the summary of recommendations available to LegCo sessions.

4.10 The Team examined the PIA summary of recommendations for SMARTICS which were published from 2001 to 2005. Specifically, the Team studied the recommendations and the ImmD's responses in respect of each PIA. The Team also checked if ImmD had taken actions as proposed in its responses.

4.11 Generally all actions proposed to be taken by ImmD were found to have been implemented. There is one action item touching upon audit trails that needs to be enhanced, and will be dealt with under DPP4 later.

Specific Findings with Potential Impacts

4.12 The Commissioner found two specific areas where improvements are required. Given these issues are related to governance, it was the Commissioner's belief that they should be accorded priority.

Data Classification

4.13 It is essential for the data user to classify information according to its actual value and level of sensitivity in order that appropriate level of controls can be deployed. A system of data classification should ideally be simple to understand and administer, so that it can be uniformly and effectively applied throughout the organization to ensure a standard level of protection.

4.14 The categories of classified information in ImmD were defined in *Chapter III of the Security Regulations of the Government*. ImmD employees were required to observe the requirements in the Security Regulations to protect classified information. ImmD had reminded its staff of the same by disseminating a circular to all staff concerned requiring them to read and understand its contents.

4.15 Nonetheless, the Commissioner considered that the classification

of personal data in SMARTICS should be more specific. Paragraph 7 of the *Information Technology Security Guidelines for SMARTICS* (“**SMARTICS Security Guidelines**”) states: “*SMARTICS contains data that are either classified as ‘RESTRICTED’ or ‘CONFIDENTIAL’. Access to the information must be properly controlled and should follow the “need to know” principle. Special attention should also be paid to the [Ordinance].*”

- 4.16 According to ImmD, “*ROP data means particulars, including photographs and fingerprints taken, furnished to a registration officer under the provisions of the ROP Regulations. ROP data are normally classified as ‘RESTRICTED’ or above*”. The Team found no detailed elaboration on the exact classification of each kind of Smart ID Card Data in all relevant guidelines of ImmD.
- 4.17 In fact, an independent auditor had conducted a security risk assessment⁵ on SMARTICS between September 2006 and January 2007 and found that “*No clear description for the CONFIDENTIAL information of SMARTICS in documentation – SMARTICS documents should be revised to describe the CONFIDENTIAL information in SMARTICS, and to provide guidelines and procedures to users for proper handling of CONFIDENTIAL information*” and recommended ImmD to “*amend the IT Security Guidelines for SMARTICS to describe the CONFIDENTIAL information and the security requirements. In addition, system manuals should also be revised to ensure that SMARTICS users are aware of the classification of information and relevant handling procedures*”. ImmD had accepted the recommendation and agreed to implement the same by the end of March 2007.
- 4.18 The Team found that the latest version (dated August 2008) of the SMARTICS Security Guidelines was not specific enough in defining under what conditions Smart ID Card Data should be

⁵ Security Risk Assessment Audit Report – Security Risk Assessment & Audit Services for the EXPRESS and SMARTICS of Immigration Department, Version 1.1, February 2007.

classified as RESTRICTED or CONFIDENTIAL. The Commissioner considered that data classification guidelines of Smart ID Card Data should be more specific.

- 4.19 **Response from ImmD:** There are already guidelines in data classification. Personal data in SMARTICS are generally classified as “RESTRICTED”. If the personal data relate to other sensitive matters such as crime investigation, a higher classification of “CONFIDENTIAL” is adopted. Taking into consideration of the Commissioner's finding, the SMARTICS Security Guidelines will be revised to provide more detailed classification of information in SMARTICS and the relevant handling procedures. Also, training and briefing will be delivered to SMARTICS users to further increase their awareness on classification of Smart ID Card Data and their protection requirements.

Objective of the Recommendation 1

Clear and easy-to-follow data classification regarding Smart ID Card Data is to be specified and promulgated to all related stakeholders so that the level of protection required on all Smart ID Card Data is easily understood and consistent.

RECOMMENDATION 1

1. Amend the SMARTICS Security Guidelines to describe the confidential information and the corresponding security requirements.
2. System manuals should be revised to document the classification of information and relevant handling procedures.
3. Conduct training and awareness programme to ensure all SMARTICS users are familiar with the classification of the Smart ID Card Data and their protection requirements.

Documentation

- 4.20 ImmD developed a Manual Procedures that included detail instructions for staff to follow in handling Smart ID Card Data.

During the Policy Review, the Team observed that the Manual Procedures was not up-to-date. For instance, Chapter 1.2 (version 2.1) of Volume II of the Manual Procedures regarding the handling of requests for Smart ID Card Data within the ROP Records Section contained the procedures for “*Requests made via the Processing Automation (PA) computer terminals*”. Despite the phasing-out of the PA computer terminals in early 2009, the latest Manual Procedures had not been amended to reflect the change.

4.21 In another example, the reporting line of the CRU mentioned in Chapter 3.2 of the latest Manual Procedures had been changed from the ROP Support Section to ROP Records Section. However, the Manual Procedures kept by the CRU did not reflect such change. The Team observed that staff members of the CRU just made hand written amendments to the Manual Procedures for their own reference. Moreover, Smart ID Card Centres, which had already ceased operation in May 2007, were still mentioned in Chapters 2.2, 2.4, 3.6 of Volume II and Chapter 3.1 of Volume III of the Manual Procedures as if they were still in operation.

4.22 The Manual Procedures must be reviewed, and updated as needed, then re-approved so that ImmD staff members know that they can rely on its contents. The dates / version reference of the reviewed and updated Manual Procedures should be clearly indicated for users’ attention. It is also helpful to the staff if the changes are identified. This can prevent documents from becoming inaccurate or obsolete over time and assist users in knowing what has changed. The above examples illustrated that ImmD’s effort in updating its operation instructions had not been sufficient.

4.23 **Response from ImmD:** There is indeed a lifecycle management relating to the review, approval, promulgation, dissemination and updating/deletion for all the documentation especially the Manual Procedures. Any revised versions of the Manual Procedures will be first put up to the senior management for endorsement and, after approval, distributed to all stakeholders for reference. All endorsed amendments or updates are centralized by a designated section (i.e. the ROP Support Section) who will take stock and

closely monitor the updates with a view to incorporating the changes and revised procedures into the Manual Procedures in a collective manner normally on a yearly basis. The quoted changes had either been consolidated by the ROP Support Section pending formal changes to take effect, or it had not been internally formalised hence it could not be updated to the Manual Procedures yet, or the section in the Manual Procedures was still required to remain for operational reasons. Taking into consideration of the Commissioner's finding, ImmD will ensure a lifecycle management mechanism is in place to be followed through by the parties concerned.

Objective of the Recommendation 2

Ensure that the lifecycle management for all the documentation including, but not limited to, approval, promulgation, regular review, version-control, dissemination and updating / deletion are followed.

RECOMMENDATION 2

To enhance a lifecycle management mechanism of all the documentation to ensure that they are regularly reviewed and updated. All changes should be clearly marked and approved. Revised copies should be distributed to all stakeholders. Replaced documents should be recalled and destroyed.

DPP1 – Purpose and Manner of Collection of Personal Data

4.24 The collection of personal data is governed by **DPP1** in Schedule 1 to the Ordinance. **DPP1(1)** stipulates that personal data shall not be collected unless the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data and the collection of the data is necessary for or directly related to that purpose. Further, the data collected are adequate but not excessive in relation to that purpose. **DPP1(2)** requires that personal data shall be collected by means which are lawful and fair in the circumstances of the case.

- 4.25 **DPP1(3)** provides that on or before a data user collects personal data directly from a data subject, the data user shall take all practicable steps to inform the data subject of whether it is obligatory or voluntary for him/her to supply the data, and if he/she is obliged to do so, the consequence for him/her if he/she fails to supply data. The data subject should also be informed of the purpose of collection and the classes of transferees of the data.

Personal Information Collection Statement

- 4.26 According to the requirement of **DPP1**, a statement should be given to data subjects during the collection of their personal data to inform them of such matters as the purpose, possible classes of transferees, rights of access and correction, and who they may contact to request for access or correction of the personal data collected. This statement is often referred as the Personal Information Collection Statement (“**PICS**”).
- 4.27 With the provision of a PICS (or a similar/equivalent document), data subjects can make an informed decision on whether they should provide their personal data to the data user.
- 4.28 Although the provision of personal data to ImmD by individuals is obligatory for registration and application for Smart ID Cards purpose under the ROP Ordinance, still it is a statutory requirement under the Ordinance for ImmD to provide a PICS to the data subjects. Applicants can therefore be assured of how their personal data would be used by ImmD and be informed of their rights to request for access and correction of their personal data.

General Comments

- 4.29 ImmD collects individuals’ personal data principally in the identity card application process. According to Regulations 4 and 4A of the ROP Regulations, every person who applies for an identity card shall furnish his personal data to ImmD. Hence, ImmD has a legal right and obligation to collect Smart ID Card Data from applicants and the kinds of personal data collected are prescribed

by the ROP Regulations for ImmD in the performance of its function of issuing identity cards. Regarding the scope of data collected by ImmD, the Team examined different kinds of identity card application forms and found that the personal data collected were in line with that required by the ROP Regulations.

4.30 ImmD’s Statement of Purpose (which served the purpose of a PICS) was printed on different kinds of identity card application forms for the attention of Smart ID Card applicants. For those individuals who also apply for optional immigration services such as Express e-Channel for passengers or e-Channel for vehicles, ImmD would inform them the respective collection purposes by a specially designed Statement of Purpose. With these practices and procedures in place, the Commissioner was generally satisfied that the ImmD had sufficiently addressed the requirement to collect Smart ID Card Data by lawful and fair means.

4.31 The Commissioner found that ImmD had generally addressed the requirements of **DPP1** (with one area that needed improvement to be discussed in paragraph 4.32 below) by providing the Statement of Purpose which informed the applicants of the collection purpose, classes of transferees, and individual’s rights of access to and correction of the personal data.

Specific Finding that Needs Improvement/Review

4.32 It is a requirement under **DPP1(3)** that where the provision of personal data by the data subject is obligatory, a data user has to inform the data subject of the consequences for him/her if he/she fails to provide the data. The consequences for a data subject who fails to supply his/her Smart ID Card Data are not spelt out in the Statement of Purpose.

4.33 **Response from ImmD:** ImmD will seek further advice from the Commissioner and Department of Justice on the necessary amendments and wordings in the Statement of Purpose.

Objective of the Recommendation 3

Data subject should be explicitly or implicitly informed, on or before collecting the Smart ID Card Data, the consequences for him if he should fail to supply the data that are obligatory for him to supply.

RECOMMENDATION 3

To amend the Statement of Purpose to include the consequences for a data subject if he fails to supply his personal data in his Smart ID Card application, in accordance with the requirement of DPP1(3)(a).

DPP2 – Accuracy and Duration of Retention of Personal Data

DPP2(1) - Accuracy of Personal Data

4.34 **DPP2(1)** stipulates that all practicable steps shall be taken to ensure that personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used.

Accuracy Checking

4.35 For the purpose of this Policy Review, ImmD is expected to have a documented system for checking the accuracy of the collected Smart ID Card Data.

General Comments

4.36 ImmD’s documentation showed that it had established distinctive roles and responsibilities for different offices and staff in ensuring data accuracy.

4.37 ImmD issued an *Immigration Services Standing Order* (“**ISSO**”), *Immigration Departmental Circulars* (“**IDC**”) and internal memoranda instructing its staff to comply with the requirements of

the Ordinance including **DPP2**. Besides, it had in place a detailed Manual Procedures stating the step-by-step procedures of different offices in handling Smart ID Card Data for its staff to follow.

4.38 The Manual Procedures required its staff to ensure the accuracy of the Smart ID Card Data collected from the applicants in every SMARTICS related function ranging from data collection to card issuance. For example, it stated that the staff of ROP Office should “*ensure the application form is properly completed and duly signed by the applicant...invite applicant to sign against the amendment*” when collecting applicants’ Smart ID Card Data.

4.39 After collecting the Smart ID Card Data from applicants, the data would be transferred to the Verification Office for fingerprint matching with the applicants’ previous records in order to ensure the accuracy of the collected Smart ID Card Data before proceeding to the card personalization process. Fingerprint matching procedures were documented in detail in the Manual Procedures which also required supervisors of the Verification Office to conduct spot checks against the verified Smart ID Card Data. In order to ensure its staff’s proficiency in fingerprint matching procedures, ImmD issued a *Brief on Fingerprint Identification Principles* for training its staff.

4.40 On top of data verification and card personalization, the Manual Procedures further required ImmD staff to ask the applicants to confirm the accuracy of the data on the identity card before issuing it at the ROP Offices.

4.41 The Commissioner was generally satisfied that sufficient details, and checks and balances, were provided in the Manual Procedures to ensure the accuracy of the collected Smart ID Card Data.

DPP2(2) – Retention of Personal Data

4.42 **DPP2(2)** stipulates that personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used.

Data Retention

- 4.43 ImmD is expected to have a retention policy and/or guidelines for its staff to follow to ensure that ImmD does not keep the data after the purpose (including any directly related purpose) for which the data were collected has been fulfilled.

General Comments

- 4.44 ImmD had a retention schedule in place designating the retention periods of different kinds of documents containing Smart ID Card Data on need basis. For instances, the schedule required that Smart ID Card Application Forms ROP 1, 2, 3 and 21b should not be kept longer than six months after registration. Similarly, any cancelled identity card returned for destruction should be kept “*until next working day after completion of all record updating*”. It further stated the retention requirement in its guidelines and procedures to facilitate its staff to follow the respective retention periods of different documents before disposal.
- 4.45 The SMARTICS Security Guidelines also stated that the keeping of individual audit trail reports “*should be in line with the specified retention period. After the retention period, the audit trail reports should be disposed of properly*”. Also, Chapter 1.1 of Volume 1 of the Manual Procedures mentioned that “*the collected ID card application forms will be retained at the office for a specified period in accordance with the Retention of Records Manual before disposed of as classified waste*” as well.
- 4.46 The process of data verification and retention requirement were also clearly defined in the Manual Procedures. The Commissioner was generally satisfied that ImmD had sufficiently addressed **DPP2** in its guidelines and procedures.

DPP3 – Use of Personal Data

- 4.47 **DPP3** provides in essence that unless the prescribed consent of the

data subject is obtained, his or her personal data shall not be used (including transfer and disclosure) for purposes other than the original purpose of collection or a directly related purpose.

Allowable Use

4.48 Under section 9(a) of the ROP Ordinance, the use of Smart ID Card Data by ImmD staff is restricted. The section states that:

“particulars furnished to a registration officer under this Ordinance may be used for and only for the purpose of enabling the Commissioner to issue identity cards and to keep records on such particulars;”

4.49 Any person who uses the Smart ID Card Data without lawful authority or reasonable excuse shall be guilty of an offence.

4.50 Moreover, ImmD should not use the Smart ID Card Data for purposes other than those mentioned in its Statement of Purpose unless with the prescribed consent of the data subjects according to **DPP3**. All these restrictions are also required to be observed by ImmD’s contractors or vendors who need to handle Smart ID Card Data when providing their services to ImmD.

General Comments

4.51 To ensure compliance with the legal requirements, ImmD issued different *Immigration Department Notices* (“**IDN**”), IDC and memoranda to raise its staff’s awareness in protecting Smart ID Card Data from unauthorized use. For examples, IDN no. 262/97 “*Personal Data (Privacy) Ordinance*”, IDC no. 44/96 “*Compliance with Personal Data (Privacy) Ordinance*”, IDC no. 7/97 “*Guidance Note on Compliance with Personal Data (Privacy) Ordinance*” and an internal memo “*Disclosure of ROP Particulars under Section 11 of ROP Ordinance*” were all related to the protection of personal data.

4.52 Under section 11 of the ROP Ordinance, with the written

permission of the Chief Secretary for Administration, ImmD may disclose the collected personal data. As delegated by the Chief Secretary for Administration, Secretary for Security has authorized the disclosure of Smart ID Card Data to government departments/ statutory bodies/ organizations/ foreign governments in a standing approval. In other words, such disclosure is lawful in accordance with ROP Ordinance. ImmD has also addressed such disclosure in its Statement of Purpose that *“the personal data furnished in the application will be used by Immigration Department ... to exercise the powers and carry out the duties under the Registration of Persons Ordinance (Chapter 177) and its subsidiary Regulations including disclosure of information as permitted in writing by the Chief Secretary for Administration by virtue of section 11 of the Registration of Persons Ordinance”*. Regarding other parties that are not within the approved list of government departments or statutory bodies, ImmD requires its staff to *“study the case and examine whether it is exempted from the provisions of Personal Data (Privacy) Ordinance [PD(P)O]”* and *“Seek legal advice where necessary”* according to the Manual Procedures.

- 4.53 On the computer system level, the Team had examined the *“Response to Tender for the Design, Supply, Implementation, Commissioning and Maintenance of and the Provision of Other Related Services for the Smart Identity Card System (SMARTICS) for the Immigration Department”*, a technical proposal from the SMARTICS service provider in response to the tender exercise of the system. It was found that ImmD had stipulated the confidentiality requirement in the tender document to protect all information, including personal data that the service provider might come into contact as part of the project.
- 4.54 ImmD had properly informed the applicants about the possible transfer of their personal data in its Statement of Purpose. Besides, ImmD had brought to its staff’s attention the legal requirements governing the use of Smart ID Card Data through a variety of internal circulars. Moreover, ImmD imposed on the third party service providers (including their sub-contractors) the obligation of protecting Smart ID Card Data from unauthorized use and

disclosure through contractual means. In this regard, the Commissioner found that ImmD had taken practical steps to prevent contravention of **DPP3** by ImmD staff, the SMARTICS third party service providers and their employees.

DPP4 – Security of Personal Data

- 4.55 **DPP4** stipulates that all practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use.
- 4.56 **DPP4** further stipulates to the effect that the level of protection measures should be proportionate to the kind of data and the harm that could result on unauthorized access, processing, erasure or use.
- 4.57 Most of the Smart ID Card Data are unique (such as fingerprint) and unchangeable (or are impractical to change, such as identity card number) for an individual. Coupled with the fact that ImmD hold such data for the entire population of Hong Kong, any mishandling or unauthorized access will have grave consequence and implication including, but are not limited to, identity theft.
- 4.58 It was against this potentially damaging background that much of the assessment efforts had been spent around this **DPP4** to examine the security measures of the information system that held the Smart ID Card Data. Inevitably during the course of the examination of the security measures of an information system, the Team had to rely on, but not exclusively, principles and techniques already developed in the area of IT security.
- 4.59 The paragraphs to follow describe the principles and techniques being used by the Team during the course of the Policy Review in the area of **DPP4** for SMARTICS.

Personal Data Security Domains

4.60 When examining personal data security documentation, the expectation is that the three specific personal data security domains are to be addressed. The three specific personal data security domains are:

- ✧ **Confidentiality**
- ✧ **Integrity**
- ✧ **Accountability**⁶

4.61 **Confidentiality** protects against the risk of unauthorized disclosure of Smart ID Card Data. Confidentiality controls may include, but are not limited to the following issues:

4.61.1 **Physical Access Control**

Physical access means access to personal data that is in physical forms (such as Smart ID Card application forms, reports, or ImmD office area where Smart ID Card Data are kept). In the case of electronic data, it means access to computers, servers or networks that process/hold the Smart ID Card Data. Physical access control is the most basic control to deny unauthorized access to personal data. Whatever form the data exist, access control is about ensuring access is on a “need-to-know” basis (otherwise also known as “least-privileged access” principle). Controls in this area need to be formal, documented and reviewed regularly.

4.61.2 **Logical Access Control**

Logical access control is a more abstract concept and applies primarily to electronic data. It concerns “logical” controls/issues such as whether access to

⁶ CIA (confidentiality, Integrity and Availability) is a commonly accepted notion in IT security. However, in the context of personal data security, the emphasis is slightly shifted with Accountability (as opposed to Availability) taking a more prominent place as a major security domain.

information system is authorized formally, whether an account is created in the information system to allow for access. Furthermore, what other controls (read-only access, ability to alter data, which part of the whole data set can be read/alterd, restriction on time-of-day access, restriction on location of access, mandatory password complexity requirement, periodic password expiry forcing change of passwords, “back-door” system access, etc.) are in place to ensure access is provided and reviewed based on the same “least-privileged access” principle mentioned before.

4.61.3 **Control Measures on ‘Non-Production’ Systems**

Smart ID Card Data do not necessary exist only in the information systems where a range of access controls can be applied. Where applicable, the same data, or a portion of the same data, may exist in other “shadow” systems that the same controls may not apply or be applicable. Examples of this include backup tapes, removable processing or storage media, decommissioned systems, development or testing environments. It may not be possible to apply the same level of control over these systems/media so similar controls may have to be developed to meet specific needs.

4.61.4 **Encryption**

Encryption is often considered as another line of defence in the event that access control to Smart ID Card Data is compromised. If data are encrypted to an unreadable manner and cannot be decrypted without specific knowledge, it protects the data even when it is fallen victim of unauthorized access. In addition to whether encryption is necessary in a given case and what encryption algorithm⁷ is in use, another major

⁷ The complexity of the mathematical equation to transform the data.

consideration on the use of encryption is the management and safekeeping of the encryption key⁸. Given the sensitivity of Smart ID Card Data and the fact that the data covers the entire population, it is highly desirable that encryption is used to protect the Smart ID Card Data where appropriate.

4.62 **Integrity** refers to the risk of unauthorized alteration of Smart ID Card Data. Integrity controls may include, but are not limited to the following issues:

4.62.1 **Access Control**

The same principle of “least-privileged access” applied previously under Physical and Logical Access Control also applies here, with the shift in emphasis on the controls and risks associated with not only access, but also the ability to alter Smart ID Card Data.

4.62.2 **Segregation of Environments**

In a complex system such as SMARTICS, care should be taken to ensure that the production system data are not wrongly altered when it is mistaken as the testing or development environment. Furthermore, the recovery/resumption procedure needs to take care of situation where the backup data are updated during disaster and need to be synchronized back to the production. The segregation and independent controls of these various environments are therefore important to ensure the accuracy of data.

4.62.3 **Data Availability**

Within the context of privacy protection and the use of information system, data availability can be considered

⁸ Encryption key is the specific knowledge, usually in the form of a string of characters or codes, with which decryption can be performed to convert encrypted information to its original form.

as part of the integrity control as the loss or partial loss of the information system may lead to inaccurate data. Given the heavy use of information technology in SMARTICS, the business resumption plan/strategy needs to be formalized and promulgated to all related stakeholders to cater for events of system failure or disaster. Finally, rehearsals need to be performed to ensure such plan works and data accuracy is maintained at all time.

4.63 **Accountability** ensures that all the access and/or alteration to data is traceable to a single user or process in order to establish responsibility. Controls in accountability may include, but are not limited to the following areas:

4.63.1 **Audit Trails**

Given the sensitivity of the Smart ID Card Data, access logging in the form of audit trails is expected as part of the controls. Audit trails ensure traceability and accountability as to what time/date someone has accessed which piece of Smart ID Card Data, and can also be used to detect unauthorized access. However, access logging would only be effective if the logs contain sufficient details, are reviewed and acted upon regularly.

4.63.2 **Shared Access**

If access to an information system is shared by a group of users, the accountability will be lost. Sharing of accounts may be due to technical reasons (if the information system only allow one specific account to be created/used) or human issue (an account holder deliberately shares his/her own dedicated/personal account). Procedures or processes, either technical or administrative, need to be in place to re-establish accountability or to prevent sharing of accounts in these

cases.

4.63.3 **Third Party Service Providers**

The development and maintenance of SMARTICS involve the provision of service by third party service providers so measures must be taken to ensure all the controls put in place are all applicable to, and are being followed by, the third party providers. This may be done via contractual and procedural means.

General Comments

4.64 The *Information Technology Security Policy for ImmD* (“**IT Security Policy**”) addressed security considerations in the following nine areas:

- ✧ Organization
- ✧ General Policy and Basic Guidelines
- ✧ Physical Security
- ✧ Access Control Security
- ✧ Data Security
- ✧ Application Security
- ✧ Network and Communication Security
- ✧ Security Incident Management
- ✧ Security Risk Assessment and Auditing

4.65 The *Information Technology Security Guidelines for ImmD* (“**IT Security Guidelines**”) elaborated on the overall responsibilities and procedures to ensure the confidentiality, integrity and availability of information systems and computer data in ImmD.

4.66 As mentioned previously, it was not the Team’s expectation to be able to compare like-with-like the ImmD documentations against the security domains outlined earlier in this chapter. It was acknowledged, for example, the nine areas under the IT Security Policy covered similar areas the personal data security domains tried to address.

- 4.67 ImmD drafted the IT Security Policy based on the Baseline IT Security Policy of Office of the Government Chief Information Officer (“**OGCIO**”). Policies, guidelines and procedures examined have all been issued to ensure staff’s compliance with the privacy related legislations and regulations when performing their duties.
- 4.68 ImmD issued many internal circulars, memoranda and e-memos for staff on a regular basis reminding them to ensure personal data security. For example, all service grade staff were required to confirm with their signatures that they had read and understood the privacy related internal circulars and memoranda.
- 4.69 ImmD also disseminated other security related circulars and memoranda to staff by circulation of hard copies and posting them on ImmD’s Intranet portal.
- 4.70 Based on the documentations provided by ImmD, the Commissioner was generally satisfied that no major issue was found (with two areas which require further enhancement) with regard to the completeness of the documentations in covering the three personal data security domains – **Confidentiality, Integrity and Accountability**.

Specific Finding with Potential Impact

- 4.71 The Commissioner, however, found an area in the documentation where further enhancement is required. The following finding is considered as having potential impact and should be accorded priority.

Audit Trails

- 4.72 The fourth PIA of SMARTICS report recommended ImmD to provide additional training and support to strengthen staff’s awareness in personal data protection with respect to how to review the audit trail reports of SMARTICS effectively and

consistently. In response to the PIA’s recommendation, ImmD agreed to “*provide further guidance on the review of audit logs, guidelines have been issued to section heads or officers in charge of the user sections/ offices in May 2004.*”

4.73 However, ImmD could not provide the specific guidelines referred. Instead, the Team was advised that the guidance was provided in the SMARTICS Security Guidelines, in which paragraph 14.10 stated: “*Section Heads and Oi/c should conduct checks on the system security audit reports including the User Management Transaction Summary and Authentication Failure Summary... They should investigate any invalid log-on events detected, seek explanation from concerned officer and take appropriate action*”. Although sample templates were shown, the Commissioner was not satisfied that this had achieved the same objective of having a dedicated guideline on how to review audit trails effectively and consistently.

4.74 **Response from ImmD:** Guidelines on checking audit trail reports are available in SMARTICS Security Guidelines and SMARTICS Manual Procedures, Volume I Chapter 11.11, Volume II Chapter 4.1 and Volume III Chapter 7.1. With these guidelines, the mechanism of conducting checks on audit trails has been running effectively over the years. Taking into consideration of the Commissioner's finding, more specific and consistent guidelines will be provided to section heads or officers-in-charge of user sections/offices to facilitate a more effective checking of audit logs for identifying irregularities. Training and awareness programs will also be arranged as required.

Objective of the Recommendation 4

To ensure the effectiveness of audit log reviews with regard to identifying inappropriate rights of access and unauthorized access.

RECOMMENDATION 4

1. To provide specific, effective and consistent guidelines to reviewers so that they can routinely and consistently conduct effective checks for identifying inappropriate access rights and unauthorized access.
2. To conduct training and awareness programmes to ensure that all audit log reviewers are familiar with the procedures on how to conduct the necessary effective checks.

Specific Finding that Needs Improvement/Review

- 4.75 The specific finding in this section may not pose an immediate impact when compared with the one listed above. Nevertheless, this finding does have implication to the security of Smart ID Card Data and therefore should be addressed.

Logical Access Control

- 4.76 System documentation is important and an organization should develop and implement a policy to ensure that the documents are kept up-to-date and consistent with each other at all times. However, the Team noted that there was inconsistency in the standards of password management between the general IT Security Policy and the specific SMARTICS Security Guidelines.
- 4.77 Paragraph 8.6.6 of the IT Security Policy stated “*Users shall change their passwords at least once every three months or whenever deemed necessary.*” whereas paragraph 14.6 of the SMARTICS Security Guidelines did not follow this more authoritative policy and stated a lesser requirement of “*Passwords for SMARTICS users are valid for six months*”.

- 4.78 **Response from ImmD:** Taking into consideration of the Commissioner's finding, the relevant SMARTICS Security Guidelines will be amended to be in line with the IT Security Policy that “Users shall change their passwords at least once every three months or whenever deemed necessary.” For the change in SMARTICS to oblige users to change their passwords every three months, it would take some time to implement the change.

Objective of the Recommendation 5

To ensure that consistent password expiry/change requirements are aligned with departmental and system policies/guidelines.

RECOMMENDATION 5

1. To review and determine the correct password expiry/change policy and amend the appropriate documents to reflect the agreed period of forced password change.
2. To conduct awareness programmes to ensure all SMARTICS users are familiar with the requirements.

DPP5 – Information to be Generally Available

- 4.79 **DPP5** provides that all practicable steps shall be taken to ensure that a person can ascertain a data user’s policies and practices in relation to personal data, be informed of the kind of personal data held by a data user, and be informed of the main purposes for which personal data held by a data user are or are to be used.

Communication to Data Subject

- 4.80 The ImmD is expected to make readily available all the policies, guidelines and procedures in relation to its collection, holding and use of personal data. One way to meet this requirement is to draw up statements of these matters to be provided through efficient and effective channels.

General Comments

- 4.81 The Team observed that ImmD stated in a Statement of Privacy Policy and Practices (“**Privacy Policy**”) booklet its privacy policy and categories of personal data held such as travel records, application and registration records, crime investigation, prosecution records and other records related to the operation of ImmD. Also, the Privacy Policy contained ImmD’s personal data collection purposes and practices adopted to ensure compliance with the Ordinance. The Commissioner was satisfied that the Privacy Policy had generally covered the required elements of DPP5.
- 4.82 Furthermore, to comply with the transparency principle under DPP5, ImmD provided its data protection related IDCs, IDNs and memoranda to all staff by posting them on its Intranet portal. Besides, hard copies of the circulars and memos were circulated to the staff. Although **DPP5** is about the transparency of policies and practices to data subjects, the familiarisation of ImmD staff to these policies and practices would help them communicate more effectively these policies and practices to data subjects.
- 4.83 ImmD was found to have taken reasonably practicable steps to ensure that its privacy policies were readily available to all staff members. No non-compliance by ImmD in respect of **DPP5** was revealed in the Policy Review.

DPP6 – Access to Personal Data

- 4.84 **DPP6** stipulates that data subjects should be able to exercise their rights to access their personal data held by a data user at a fee, if any, that is not excessive and to make correction if necessary.

Data Access Requests and Data Correction Requests

- 4.85 Under the Ordinance, every individual has the right to request a data user, e.g. a government department or a company, to confirm whether it holds his or her personal data and to request a copy of

any such data. Such request is called data access request (“**DAR**”). The Ordinance allows the imposition of a fee for complying with a DAR but the fee charged shall not be excessive. If the data user concerned has valid grounds to refuse to comply with the request, it should reply to the individual with reasons within the 40 days limit. If the data user concerned is unable to comply with the request within the prescribed period, e.g. due to data being stored overseas, it should inform the individual of the situation within the same 40 days period and comply with the request as soon as practicable thereafter.

- 4.86 If the personal data provided in response to a DAR are inaccurate, the data subject can request for correction of the relevant personal data by making a data correction request (“**DCR**”) under the Ordinance. Similar to DAR, the party receiving a DCR shall also respond within 40 days. If the request is complied with, the party should provide the data subject with a copy of the corrected data. If not, the party should inform the data subject why this has not been done.

General Comments

- 4.87 In relation to the DAR fee, ImmD issued an internal circular IDC no. 28/97 “*Imposition of Fees for Complying with Data Access Requests*” and an “*Internal accounting procedures for collection of charges related to Section 28 of the Personal Data (Privacy) Ordinance*”. The documents provided detailed guidelines for charging DAR fee.

Specific Finding that Needs Improvement/Review

- 4.88 Among ImmD’s internal circulars and guidelines, however, ImmD only provided general guidelines to staff in DAR and DCR by issuing the IDC no. 7/97 “*Guidance Notes on Compliance with the Personal Data (Privacy) Ordinance*” and the ISSO. For instance, ISSO states that:

“Data access requests (section 18 to 21)

(a) Section 18 to 21 of the Ordinance provide statutory requirements for data access request; compliance with data access request; circumstances in which data user shall or may refuse to comply with data access request; and notification of refusal to comply with data access request. In particular, the 40-day time limit specified in section 19(1) should be strictly adhered to.

Data correction requests (section 22 to 25)

(b) Section 22 to 25 of the Ordinance provide statutory requirements for data correction request; compliance with data correction request; circumstances in which data user shall or may refuse to comply with data correction request; and notification of refusal to comply with data correction request, etc

...

Log book for refusals of data access and correction requests (section 27)

(d) Section 27 of the Ordinance requires a data user to keep a log book to record all refusals of data access and correction requests and the particulars of the reasons for the refusals. All sections must keep and maintain such a log book.”

- 4.89 The Commissioner found that existing guidelines of handling DAR and DCR are too general.
- 4.90 Taking note of the Commissioner’s observations, ImmD subsequently issued an e-Memo on 17 May 2010 with more detailed guidelines and procedures for handling DAR and DCR (“**the New Guidelines and Procedures**”). The New Guidelines and Procedures have been issued and distributed to division / section heads and officers in charge.

Objective of the Recommendation 6

To ensure that the staff members who are charged with the responsibility of handling data access requests (DAR) and data correction requests (DCR) are familiar with the New Guidelines and Procedures for handling DAR and DCR.

RECOMMENDATION 6

To conduct awareness programmes to ensure that all staff members responsible for handling DAR and DCR are familiar with such guidelines.

Workflow Review

Workflow Review

- 5.1 The objective of the Workflow Review is to examine and assess whether all the formal policies, guidelines and procedures examined under the previous chapter are being followed. One key criterion was to look for sufficient evidence, either from documents or actual practice to assess the level of conformity.
- 5.2 Unlike the Policy Review, the Workflow Review involves more dynamic interactions with many internal stakeholders. The Team acknowledges that it is not possible for detailed procedures to be written for every single step of a workflow and interaction between stakeholders. As such, the Team must exercise judgements on the compliance level of stakeholder behaviours against policies and guidelines that are often abstract in nature.
- 5.3 The Team conducted the Workflow Review mainly by three channels: (i) observations and interviews, (ii) outcomes examination, and (iii) questionnaires and surveys.

Evidence Examined

- 5.4 During the Workflow Review, the Team conducted observations and walk-throughs in 19 ImmD offices and control points between 24 September and 15 October 2009 (**Appendix III**).
- 5.5 ImmD facilities being examined included public waiting areas at ROP Offices, service booths, processing areas, identity card production facilities, record storage and record destruction facilities, self service kiosks, SMARTICS terminals, IT server rooms and data backup facilities.
- 5.6 During this examination period, the Team observed the full cycle of identity card application from the interviewing of the applicants,

to the issuing of the identity cards. Where necessary and applicable, the Team also examined relevant records, logs and reports to ascertain the level of compliance with the requirements of the Ordinance.

- 5.7 A survey was conducted face-to-face with 333 Smart ID Card applicants between 12 and 18 August 2009 (**Appendix IV**). The survey aimed to assess from the applicants' perspective whether the data protection measures taken by ImmD in the handling of Smart ID Card Data by staff in daily work were effective. 300 questionnaires (**Appendix V**) were also handed out to ImmD staff on 4 November 2009. The questionnaires were designed to examine the level of understanding and compliance of personal data protection from the perspective of the ImmD staff. All except three questionnaires were properly completed making the total number of staff who had supplied valid answers to 297. The 300 questionnaires represented 27% of a population of about 1,101 ImmD staff who were responsible for handling Smart ID Card Data in the 16 selected offices⁹ at the material time.

Governance

- 5.8 The importance and the scope of Governance for privacy protection were described in the previous chapter. During the Workflow Review, the Team looked at the actual implementation of various controls under the category of Governance to see if the stated policies, guidelines and procedures had indeed been followed, and whether such compliance had been reflected in actions, behaviours and records.

General Comments

- 5.9 The following points are the general comments the Commissioner wishes to make on the various controls under **Governance**. Details of the findings which point to possible improvements are listed in the sections "Specific Findings" to follow.

⁹ Questionnaire exercise excluded disaster recovery centre and resilience centre from the visited offices.

- 5.9.1 **Structured Management Control** – The Commissioner found that the roles and responsibilities of all ImmD staff were defined and known.
- 5.9.2 **Privacy by Design** – ImmD appeared to have followed up all items recommended in the PIAs save as one item as listed in Chapter 4 as Recommendation 4.
- 5.9.3 **Documentation** – The relevant policies, guidelines and procedures are generally available and disseminated to all immediate and related stakeholders regularly.
- 5.9.4 **Data Classification** – Currently the data classification of information stored in SMARTICS should be more specific.
- 5.9.5 **Assessment/Audit** – The Commissioner found room for improvement on timely reporting of privacy compliance self-assessment exercise.
- 5.9.6 **Data Breach Management** – It was reported that no data breach incident of SMARTICS had ever been reported in ImmD since its launch so the Commissioner could not comment on the compliance in this area.
- 5.9.7 **Training and Awareness** – Given the length of time SMARTICS has been introduced, the frequency and scope of training could be enhanced to raise privacy awareness.

Specific Findings with Potential Impacts

- 5.10 Specific findings with potential impacts are listed in the sections to follow. Given these issues are related to Governance, it is the Commissioner’s belief that they should be accorded priority.

Data Classification

- 5.11 This is a related finding based on the Policy Review that more detailed guideline on data classification of Smart ID Card Data should be provided by ImmD. While the Commissioner noted that the majority, being 201 (68%) of the surveyed staff were able to answer that the correct classification of Smart ID Card Data was either “restricted” or “confidential”, given the high degree of sensitivity of the data, ImmD should strive to further enhance their awareness.
- 5.12 **Response from ImmD:** Taking into the consideration of the Commissioner’s finding, the SMARTICS Security Guidelines will be revised to provide more detailed classification of information in SMARTICS and the relevant handling procedures. Also, training and briefing will be delivered to SMARTICS users to further increase their awareness on classification of Smart ID Card Data and their protection requirements.

The issue of data classification was identified previously under Policy Review (Chapter 4). The finding here in the Workflow Review only reinforces this previous finding. The objective and recommendation of this specific finding repeat **Recommendation 1.**

Training and Awareness

- 5.13 A survey was conducted to ascertain the level of formal training provided to staff. In the returned staff survey, 120 respondents (40%) said that they had never attended any privacy protection training.
- 5.14 The survey also indicated that 213 respondents (72%) had failed to show an understanding of the DPPs of the Ordinance in a scenario question. Of the 213 respondents, 153 of them had served in ImmD for eight years or above.

5.15 134 respondents (45%) said they had not read all of the following major policy and guidelines, which were required to be read by all staff :

- Information Technology Security Policy for Immigration Department
- Information Technology Security Guidelines for Smart Identity Card System
- Immigration Department Circular No. 9/2008 – Compliance with Data Protection Principle 4 of Personal Data (Privacy) Ordinance
- Immigration Department Circular No. 2/2009 – Security in the Handling of Classified Documents

5.16 Section heads and officers-in-charge are allowed to access audit trail reports generated by SMARTICS. According to SMARTICS Security Guidelines, they are required to store the reports in a lockable cabinet when not in use. The reports should be disposed of after being kept for six months.

5.17 The Team acknowledges the enormous task of the ImmD to update its staff on all the personal data protection measures and recognizes the achievements so far. However, there is still room for improvement on the training provided to ImmD staff to enhance their awareness level to security/privacy protection.

5.18 **Response from ImmD:**

5.18.1 The high percentage of untrained officers may be attributed to their misconception that “training” would only mean lecturing inside a classroom while other teaching methods are not considered by them as training.

5.18.2 Since October 1995, ImmD had provided personal data protection training programmes for immigration service staff. Such training programmes were also incorporated into all induction courses for new recruits. The Immigration Service Institute of Training and Development of ImmD has organized a total of 96 in-

service courses on personal data protection with 2,503 officers, and 2,539 officers having received such training in the induction training.

- 5.18.3 On-the-job training by means of workshop, circulation of guidelines / instructions, briefing and sharing with experienced officers, was also provided to staff.
- 5.18.4 Since 2003, the Records of Data Management Section of ImmD has been making arrangements for ImmD staff to attend the “Seminar on Introduction to the Personal Data (Privacy) Ordinance” organized by the PCPD.
- 5.18.5 Training materials are readily available for the staff who should be well aware of the prevailing policies and guidelines on privacy protection. Information on privacy protection is available on Intranet Portal for staff’s reference. Memos / Circulars are issued periodically to inform and remind staff of matters relating to the handling of personal data under the Ordinance.
- 5.18.6 ImmD will consider organising more in-house training, lectures and seminars for the staff.
- 5.18.7 Respondents who answered that they had not read the specified policy and guidelines might have been caused by the lapse of the staff’s memory on the titles of the related notices / guidelines.

Objective of the Recommendation 7

To ensure that training and awareness programmes contain sufficient depth on personal data protection, and that these programmes are effectively delivered.

RECOMMENDATION 7

To consider and review the current arrangement of staff-training so that more staff can participate and the training program may become more effective.

Assessment/Audit

- 5.19 It is the Government's policy that security audits should be carried out periodically to monitor the compliance of security risk. At ImmD, three IT Security Audits were conducted biennially in 2005, 2007 and 2009 by OGCIO and other IT consultancy firms.
- 5.20 ImmD has in place policy and practice to carry out reviews on daily operational procedures for the purpose of detecting irregularities, e.g. by examining spot check registers and audit trail reports. Section heads or officers-in-charge are delegated with the authority to perform the review. Spot check system has been adopted by ImmD to ensure that all requests for provision of Smart ID Card Data are handled in accordance with the established policies and procedures.
- 5.21 Two privacy compliance self-assessment exercises were conducted in November 2005 and December 2008 respectively. The exercises were conducted in accordance with the Privacy Assessment Checklists, which were developed to fit the operational processes of respective SMARTICS units, and served as a tool for internal audit. Guide for Privacy Compliance Self-assessment Exercise was issued for the first exercise to facilitate sub-division heads to perform the audit.
- 5.22 The results and findings of the exercises were forwarded to the

Principal Immigration Office (Records and Data Management) for comments. As communication issue among departments and units was revealed in the first self-assessment exercise, ImmD increased its efforts to raise awareness and executing measures to address the issue. The checklists were revised and consolidated again for the second exercise.

5.23 Nevertheless, the Team noted that considerable time was spent on the compilation and communication of the final reports, which probably affected the timing and effectiveness of the follow-up actions. The Team was told that the report of the first exercise was distributed to respective division heads in December 2006 and the report of the second exercise was still being prepared in January 2010 for dissemination to respective division heads and user sections. Through further enquiries, the Team understood that interim feedbacks of the second exercise were provided to user sections in July 2009 which is an improvement from the first exercise in terms of the speed of providing feedback.

5.24 **Response from ImmD:** There was no delay in the release of the self-assessment results as well as the timing and effectiveness of the follow-up actions. Two Privacy Compliance Self-assessment Exercises were coordinated by ROP Division of ImmD in November 2005 and December 2008 respectively, which served as internal audits on the privacy compliance measures of all Smart ID Card Data users of ImmD. Moreover:-

5.24.1 For the 1st Exercise, a total of 154 sets of Privacy Self-assessment Checklists were compiled by respective Smart ID card data users and consolidated by the ROP Support Section in January 2006. For any case of irregularities observed during the exercise by the user sections, immediate action would be taken to address the situations promptly with details duly reported in the checklists. The completed checklists, after consolidation of findings and analysis, were then forwarded to an independent advisor / auditor on privacy matters of the Department i.e. Principal Immigration Officer (Records

and Data Management) (“**PIO(RM)**”) for examination in May 2006. PIO(RM) gave his observations to the ROP Support Section in June 2006 after a thorough study on the self-assessment results. While it was viewed that the exercise was conducted properly and all sections concerned had generally fulfilled the requirements as stipulated under the 6 DPPs, PIO(RM) also offered his views for improvement of the exercise and rectification of other discrepancies identified in the self-assessment checklists. The assessment results with the observations from PIO(RM) were then disseminated to the relevant users in September 2006 for information and follow-up action accordingly. Upon completion of all follow-up actions by sections concerned, the report was then finalized and delivered in November 2006. As such, the final report had indeed embodied all aspects of the exercise from the beginning till the completion of all actions, and there was no delay caused to the timing and effectiveness of the follow-up actions.

- 5.24.2 For the 2nd Exercise in December 2008, a total of 136 sets of Privacy Self-assessment Checklists were compiled by respective Smart ID card data users and consolidated by the ROP Support Section in February 2009. Same as the 1st Exercise, immediate actions were taken by the user sections in case of any irregularities observed during the exercise with details duly reported in the checklists. All the completed checklists and the consolidated findings and analysis were then forwarded to PIO(RM) for examination in March 2009. PIO(RM) delivered his observations in May 2009 after studying the self-assessment results. PIO(RM) also viewed the 2nd Exercise was conducted properly and all sections concerned had generally fulfilled the requirements as stipulated under the 6 DPPs. The assessment results and PIO(RM)’s observations were then disseminated to all users concerned in July 2009 for information and follow-up action. Upon completion of all follow-up

actions by sections concerned, the report was subsequently finalized and delivered in February 2010. There was no delay caused to the timing and effectiveness of the follow-up actions as the final report of 2nd Exercise had actually covered all aspects from the beginning of the exercise till the completion of all actions.

- 5.24.3 Throughout the process of both exercises, the results of the self-assessment exercises had been disseminated to all users in a reasonable, effective and timely manner. Any possible irregularities were rectified immediately upon self-evaluation and/or upon receipt of the comments from the independent auditor i.e. PIO(RM). The finalized reports merely served as a documentation to record all the details and course of action taken in the exercises and no adverse effect / impact whatsoever was caused to the follow-up actions of the user sections throughout the self-assessment exercises.

Objective of the Recommendation 8

To ensure that the results of privacy compliance self-assessment exercises are compiled and disseminated in a timely manner to maintain effectiveness of the assessments.

RECOMMENDATION 8

To consider resources and methodology to speed up the documentation process of reporting results of the privacy compliance self-assessment exercises.

DPP1 – Purpose and Manner of Collection of Personal Data

General Comments

- 5.25 The Team observed ImmD staff handling applications of Smart ID Card at various ROP Offices. Statement of Purpose (the ImmD

equivalent of the PICS) which explained the collection purpose, classes of transferees and access to personal data, were generally put up in poster form at prominent public areas of the offices. In addition, the Statement of Purpose was printed on the overleaf of application forms distributed at the offices to draw applicants' attention. When applicants were invited for interviews, some Registration Officers would brief them the Statement of Purpose again. In the survey of Smart ID Cards' applicants, 57% of them responded that ImmD staff had voluntarily explained the contents of Statement of Purpose upon collection of personal data for application.

5.26 In the collection of personal data of Smart ID Card holders for Express e-Channel for passengers or e-Channel for vehicles, applicants were provided with another Statement of Purpose and asked to confirm their understanding. Specific consents from the card holders were requested to transfer card face data and fingerprint to back end server at control points. Statement of Purpose is also widely communicated with potential applicants via posters and leaflets at Control Points. Applicants are not obliged to provide personal data if they do not opt in using the express services.

5.27 Based on the above observations, non-compliance was generally not found in ImmD with regard to **DPP1**.

DPP2 – Accuracy and Duration of Retention of Personal Data

DPP2(1) - Accuracy of Personal Data

General Comments

5.28 The workflow of processing Smart ID Card's application was designed with verification of collected data at different stages and supported with segregation of duties to ensure cross-checking. First of all, applicants' personal data were verified by ACO and IO respectively at ROP Offices before passing on for more intensive

verification.

- 5.29 To enhance the accuracy of the collected data, the Verification Office was established to perform the function of counterchecking applicants' personal information. Automatic fingerprint matching function was embedded in the SMARTICS process to provide high-score or low-score matching results against the image captured in the previous identity card application. The low-score ones would be further scrutinized on manual biometric verification including fingerprint, portrait photo and documents by senior staff. The Team found that Verification Office would withhold applications from Card Personalization Office should there be any doubt on data accuracy. Before the personalized cards were dispatched to Originating ROP Offices, there was quality check to ensure accuracy.
- 5.30 When the applicants collected their Smart ID Cards at the ROP Offices, ImmD staff would conduct a Chip test by requiring the applicants or their guardians to view and confirm the Smart ID Card Data stored on Chip. For those Smart ID Cards collected by authorized representative of the applicants, ImmD would request the applicants to check the Smart ID Card Data stored on Chip at ImmD's self-service kiosks afterwards.
- 5.31 The Team verified that Senior Immigration Officers at respective offices have conducted random checks. After examining the spot check register, it was demonstrated that the recommended target of conducting 5% manual checks by senior staff has been achieved at Verification Office for the handling of first-time application without previous registration records. ImmD has voluntarily performed security spot check although it was not required by the Security Regulations as issued by the Government.
- 5.32 The observation at Airport Control Point confirmed that Duty Officers would verify the identity (including fingerprints) of cardholders who reported loss of Smart ID Card to ensure accuracy of personal data prior to the issuance of the temporary document for re-entry.

- 5.33 In general, the Commissioner did not find any major issue relating to **DPP2(1)** in the handling of Smart ID Cards by ImmD staff in the offices and processes examined, save as one area to be discussed in the following sections.

Specific Findings that Need Improvement/Review

- 5.34 CRU handles requests for Smart ID Card Data from other government departments. There are an increasing number of requests for ROP Data from the Tobacco Control Office due to the increasing number of prosecutions under the Smoking (Public Health) Ordinance (Cap. 371). However, the frequently requested field, i.e. “address”, could not be singled out from the scanned Smart ID Card application form stored in SMARTICS. CRU staff members, therefore, need to print an image of the full application form from SMARTICS to obtain this single item from the printout.
- 5.35 CRU staff members were fully aware that the full information on the scanned application form could not be sent out to avoid disclosure of excessive personal data. They therefore manually cut the addresses from the printouts and pasted them onto the reply letters before sending them to the Tobacco Control Office. The existing measure to avoid mismatching of data subjects’ addresses is to compare the handwritings of the detached portion with the handwriting of the remaining printout by the supervisors before replies are sent out.
- 5.36 Although the data subjects’ addresses are not part of the Smart ID Card Data within the scope of this PCA, the Commissioner is of the view that this can still be a potential issue. Apart from the possible data accuracy issue in the event of mis-pasting the wrong address, the Commissioner is equally concerned about the unnecessary production of an image of the original application form (the unused classified wastes) when only a small part is required. Furthermore, the access to the applicants’ forms was found in the audit trail as a record of “full access”, which has not reflected the true nature of the access.

5.37 **Response from ImmD:** In releasing personal data to the requested departments, all CRU staff members are fully aware that they should ensure that the requests are lawful in accordance with section 11 of the ROP Ordinance, Cap.177, and no excessive data are disclosed. While all the CRU staff members are Confidential Assistants who are well versed with the confidentiality requirements in handling ROP records / personal data related to the confidential correspondence with other government departments, the officer-in-charge of CRU i.e. Senior Confidential Assistant (“SCA”) would also conduct a 100% counter-check on the reply memos/letters prior to sending out. The SCA would countercheck and ensure that (i) the retrieval of ROP records is proper and appropriate in accordance with the legal requirements; (ii) no excessive data is disclosed; (iii) the provision of “address” is correct and no mis-pasting occurred; (iv) the remaining portion of printouts of the form is properly disposed of (as confidential waste). So far, no inaccurate release of ROP data was found or reported by client departments. Besides, given the access to SMARTICS by the Confidential Assistants are governed by access rights and the office of CRU is a confined area with high security standards i.e. iron bars and strong room doors etc, there are sufficient safeguards on the security of records. That said, further system enhancement will be explored to streamline the automated process especially in the retrieval of “address” for automatic-pasting in the prescribed reply memos/letters to the client departments. Corresponding audit trial report will also be enhanced to reflect the practice for record-keeping and monitoring purpose.

Objective of the recommendation 9

To review and refine the current practice in the CRU so that only relevant information will be retrieved from SMARTICS.

RECOMMENDATION 9

1. To review the workflow and the needs for the CRU to access various data fields in SMARTICS with a view to eliminating the need for cutting and pasting information.
2. To review whether the current practice of printing the original identity card application form is the best option to meet the requests for provision of identity card holders' addresses.

DPP2(2) – Retention of Personal Data

General Comments

- 5.38 At ROP Offices, the Team noticed that cancelled Smart ID Cards were collected and would not be kept longer than necessary. They were shredded (Picture 2 in **Appendix VI**) as soon as practical or usually by the next working day.
- 5.39 The Team was impressed during the visit to the Records Provision Unit (“**RPU**”) that documents, including audit trail reports, were packed and labelled with types and dates in sequence so as to schedule for disposal according to retention period. Similar good practice also appears to exist in ROP Hong Kong Office in storing application forms and in Airport Control Point in keeping audit trail reports.
- 5.40 Airport Control Point further maintained a logbook to record the retrieved ROP enquiries and remark whether the hardcopies were destroyed in order to ensure those records would not be kept

longer than they should be.

- 5.41 The Commissioner found ImmD to have generally complied with **DPP2(2)**.

DPP3 – Use of Personal Data

General Comments

- 5.42 Under section 9 of the ROP Ordinance, Smart ID Card Data may only be used for the purpose of enabling the Commissioner of Registration to issue identity cards and to keep records on such data. The records may be used for the purposes as authorized, permitted, or required by or under any ordinance.
- 5.43 Section 11 of the ROP Ordinance stipulates that staff of ImmD are not allowed to disclose the Smart ID Card Data unless with the written permission of the Chief Secretary for Administration, who must state the reason for giving such permission. In general, such power is delegated to the Secretary for Security who will issue a standing approval to ImmD on the disclosure of Smart ID Card Data.
- 5.44 Based on the observation of the Team at RPU and CRU, staff was aware of the standing approval from the Secretary for Security. Staff of CRU would verify signatures and names of requestors while a SCA would countercheck the Smart ID Card Data to avoid excessive disclosure prior to sending out the requested information. In addition, proper authorisation and segregation of duties were found in place at these two units.
- 5.45 Under section 58 of the Ordinance, personal data are exempt from the provision of **DPP3** in cases in which the use of the data is for any of the specified purposes such as the prevention or detection of crime and the apprehension, prosecution or detention of offenders, etc. and that the application of **DPP3** would be likely to prejudice the purposes.

- 5.46 In handling urgent requests from the Hong Kong Police Force (“**Police**”), Smart ID Card Data would be transferred to the designated regional consoles of the Police for anti-crime purposes. ImmD disclosed Smart ID Card Data to the Police mainly through the predefined Secured Document Delivery System. The Police has end-to-end encrypted fax lines installed at RPU and CRU to facilitate secured electronic communication of the Smart ID Card Data. This arrangement also exists with the Independent Commission Against Corruption who has similar requests for Smart ID Card Data. Printouts of the requested Smart ID Card Data may also be collected in person by authorized members of the requested parties or sent under the Confidential Cover for official dispatch.
- 5.47 SMARTICS Controller confirmed that contractors of SMARTICS would not be assigned with any SMARTICS account. Any maintenance of the SMARTICS programmes must go through a formal change management process. Access to the production SMARTICS were carried out with the escort of ImmD staff who would log on with their own user identity captured in audit logs. The ImmD staff would monitor the whole maintenance/change process. There was little opportunity for contractors to view, acquire or change Smart ID Card Data throughout the operation.
- 5.48 It was found that the use of the Smart ID Card Data was in accordance with its Statement of Purpose and adhered to all relevant ordinances. The Commissioner did not find any non-compliance in this aspect.

DPP4 – Security of Personal Data

General Comments

- 5.49 As discussed in the last Chapter, **Confidentiality**, **Integrity** and **Accountability** are the three personal data security domains that underpin DPP4. The Workflow Review on the security protection of the Smart ID Card Data was therefore carried out according to these domains.

5.50 The following paragraphs are the general comments after the Workflow Review on the personal data security domains was conducted. Details of the findings which point to possible improvements are listed in the sections “Specific Findings” to follow.

5.51 **Confidentiality, Integrity and Accountability**

5.51.1 **Access Control** - A high level of physical access control was observed by the Commissioner with only two issues regarding the physical layout of two ROP Offices and self-service kiosks. On logical access control, there is a good segregation of duty in the user account handling process. However, the authentication method used by ImmD staff to return captured Smart ID Cards in self-service kiosks to owners did not appear to have followed the guidelines. The guidelines requiring the access right for staff who are on leave to be temporarily disabled were not followed. Password policy was found to be inconsistent at departmental and system levels. The role-based access model appears not to have been reviewed since the launch of SMARTICS.

5.51.2 **Control Measures on ‘Non-Production’ Systems** – There was a discrepancy between the computer-generated recall report and the actual location of three offsite backup tapes.

5.51.3 **Encryption** – Although the Government Security Regulations do not require Smart ID Card Data, which is classified as RESTRICTED, to be encrypted at all time, it is still highly desirable that encryption is deployed where necessary to protect such sensitive data. It is understood that ImmD was implementing the desirable encryption requirement of the Security Regulations 366 (a) on removable media.

- 5.51.4 **Segregation of Environments** – All environments are segregated and independently controlled. There is no “life/real” personal data stored in testing/development system.
- 5.51.5 **Data Availability** – The Business Resumption Plans were drawn up and found to be rehearsed regularly.
- 5.51.6 **Audit Trails** – More specific guideline on audit trail checking for irregularities is recommended.
- 5.51.7 **Shared Access** – There was no evidence to suggest that shared access to SMARTICS took place.
- 5.51.8 **Third Party Service Providers** – Data protection clauses are built in contracts. Third party service provider performance is monitored continuously and reviewed formally every six months.

Specific Findings with Potentially High Impact

- 5.52 The order of findings in this Report is based on the severity of potential impact. In general, issues that may potentially lead to personal data being accessible by external parties are considered to have higher impact over issues that may only involve internal access. Similarly generic or systemic issues have higher priority or take precedence over issues that are related to a smaller or specific area.
- 5.53 The following items are considered as having potential impact and should be accorded priority.

Control Measures on ‘Non-Production’ Systems

- 5.54 In the event of a disaster such as a fire, it is possible that all data maintained at a facility could be destroyed. ImmD reduces this risk by relocating/storing backup tapes of Smart ID Card Data at offsite facilities.

- 5.55 During the Workflow Review, the Team observed the process of delivering backup tapes of Smart ID Card Data from ImmD headquarters to an offsite backup office. The backup tapes were delivered in a locked metal briefcase (Picture 3 in **Appendix VI**) and the keys were kept by two Computer Operators, who were responsible for the daily delivery process.
- 5.56 At the offsite backup office, the Team noted that three backup tapes, which were supposed to be “recalled” from the backup office to the headquarters for recycle use, could not be located in the backup office. According to a computer-generated report, the three backup tapes should have been available in the backup office.
- 5.57 In response to the Team’s further enquiry, ImmD located the three backup tapes from a pool of “scratch” tapes in the headquarters. ImmD explained that the discrepancy between the report and the actual location of the tapes was caused by a software error of the recall system. ImmD reported that it discovered this possible issue in August 2009 and started a monitoring process to ascertain the extents of the issue.
- 5.58 Paragraph 7.4.3 of the IT Security Policy states: *“Movement of media shall be properly recorded. Periodic inventory check shall be conducted to detect any loss or destruction”*. Given the background of this incident and the sensitivity of Smart ID Card Data, the Commissioner recommends that the movements of backup tapes are rigorously monitored and the software error is fixed as soon as possible.
- 5.59 **Response from the ImmD:** The three backup tapes were confirmed to be located at the headquarters’ Computer Room so it was not a case of missing tapes. The software error appeared to have repeated the recalling of the same tapes hence tapes could not be located in the backup centre when they appeared in the recall list the second time. The issue was known in August 2009 and was fixed in December 2009. In the meantime, a standing instruction had been issued for handling the known discrepancy scenario.

Taking into consideration of the Commissioner's finding, the ImmD confirmed that the software error was fixed and tested in December 2009. The movements of backup tapes will be rigorously monitored and current guidelines and procedures will be beefed up where necessary.

Objective of the Recommendation 10

The movements of backup tapes need to be rigorously monitored.

RECOMMENDATION 10

1. To review the current guidelines and procedures to ensure the movement of backup tapes are protected and recorded.
2. To continue to monitor the accuracy of the recall system to ensure that the same error will not happen again without being undetected.

Access Control

- 5.60 In the process of a Smart ID Card application, the applicant is required to fill in an application form and submit it to an ACO at one of the ROP Offices. The ACO sitting in his/her booth will interview the applicant, collect personal data from the applicant for identity card registration, check the applicant's identity and capture the applicant's fingerprint data and facial portrait. After that, the applicant will wait for an IO's assessment at a waiting area.
- 5.61 During the Workflow Review, the Team visited five ROP Offices. At the ROP Hong Kong Office and ROP Fo Tan Office, the Team observed that people sitting in the waiting area was able to hear clearly the conversations between the applicants and ACO sitting in their booths. The open design of the booths may have posed a potential privacy risk. In fact respondents from both staff and applicant surveys suggested that ImmD should install a door at each booth.

5.62 **Response from ImmD:**

- 5.62.1 The personal data required for Hong Kong identity card registration is normally furnished on the application form and supporting documents provided by the applicants. Throughout the process of identity card applications at the registration booth of ROP Offices, staff of ImmD will normally refer to the application form and supporting documents for capturing the data and seldom raise discussion on any sensitive personal data. The conversation between staff of ImmD and the applicants are mainly clarification on the documents/data required, giving directions for capturing thumbprints and portraits, informing the following procedures/date of collection etc. For cases involving sensitive issues, e.g. change of sex, the applicant will be invited to a private room for interview/assessment before the normal registration process at the registration booth.
- 5.62.2 The existing design of the registration booths at the ROP Offices has taken into consideration of the accommodation constraints, transparency of process, need of supervision, privacy protection as well as security of the customers and our staff, where it is essential for ImmD to strike a good balance of these factors and concerns. Nevertheless, given the suggestion of the Commissioner on the sound insulation of our booths, the Director of Immigration will consider improving the design and layout in future, subject to the prevailing regulations governing the set-up of government offices, funding arrangements and availability of premises etc.

Objective of the Recommendation 11

To ensure sensitive personal data exchanged in the conversation between an applicant and the ImmD staff during an identity card application is not overheard by unrelated parties.

RECOMMENDATION 11

The ImmD to consider improving the sound insulation of the booths in ROP Offices to ensure that an adequate level of privacy is provided to identity card applicants.

- 5.63 Self-service kiosks have upright screens attached with filters limiting the viewing angle of the screens. This only allowed the users standing in front of the kiosks to view their own personal data on the screens. Some ROP Offices had their kiosks placed in locations that could prevent others in the queue from viewing the personal information of the user.
- 5.64 However, ROP Kowloon Office and ROP Yuen Long Office lined up their kiosks together (Picture 4 in **Appendix VI**). Such arrangement might allow the users of the kiosk at the back to view the personal data on the screen of the kiosk at the front. The positioning of self-service kiosks at ROP Kwun Tong Office was better to protect data privacy of users (Picture 5 in **Appendix VI**).
- 5.65 **Response from ImmD**: All self-service kiosks in the ROP Offices were installed with screen protector with view angle protection (around 45°). The on-screen data could only be viewed by the user standing right in front of the kiosk and it was difficult if not impossible for other unrelated persons to view the data from other positions. Owing to the accommodation and layout constraints of ROP-KO and YLO, the two kiosks in these offices were positioned in a consecutive way along a single line. However, the on-screen information of the front kiosk could hardly be viewed by the user at the back kiosk as the information were protected by screen protector and also blocked by the body of the front user.

Nevertheless, taking into account PCPD’s suggestion, ImmD will consider adjusting the position of the self-service kiosks in future to prevent any possible viewing by unrelated persons.

Objective of the Recommendation 12

To ensure that sensitive personal data displayed on self-service kiosks cannot be viewed by unrelated parties.

RECOMMENDATION 12

ImmD shall consider adjusting the position of self-service kiosks in future to prevent Smart ID Card Data from being viewed by unrelated persons.

- 5.66 ImmD emphasized access to SMARTICS is only granted to authorized officers. The access for SMARTICS is based on a role-based access model meaning each SMARTICS user must belong to one of the pre-defined groups (like a job role/function) called User Transaction Group. Once a user belongs to a User Transaction Group, specific access to SMARTICS is granted according to that group’s privileges. The mapping between User Transaction Group and the access to SMARTICS is documented in a spreadsheet called Security Matrix.
- 5.67 This role-based access model is a common access control model to ease the complexity of managing each officer’s access individually. A simple access model will also help to avoid mistakes.
- 5.68 The Team noted that versions of the Security Matrix obtained from the ROP Offices and Control Points looked different with different User Transaction Groups listed. Since there was no version number on the Security Matrix, it was unclear if these offices were showing the same version of the Security Matrix.
- 5.69 As a tool for user access control, clear stating of the version number and distribution mechanism of the Security Matrix are important for users to ascertain that they have the most up-to-date

version consistently used and adopted by the authorized officers.

- 5.70 **Response from ImmD:** Previous versions of the Security Matrix was inadvertently retrieved in a rush to the Team. SMARTICS Controller is at all time maintaining the most updated and unique master Security Matrix.

Objective of the Recommendation 13

A formal versioning and distribution mechanism for the role-based Security Matrix will help to ensure that all users are referring to the correct version of the Security Matrix.

RECOMMENDATION 13

To develop a formal versioning and distribution mechanism for the role-based Security Matrix in order to ensure that the correct version is distributed to and used by all the relevant parties.

- 5.71 Access to SMARTICS is controlled by user IDs and corresponding passwords. Paragraph 9.2 of the IT Security Guidelines states: *“For users who are on leave, the profile of their User IDs will be updated such that during the leave period, these users cannot have access to the System. All accounts shall be revoked after a predefined period of inactivity.”*. Paragraph 14.4 of the SMARTICS Security Guidelines also states: *“Section head and officer-in-charge should perform user assignment or un-assignment as appropriate”*.
- 5.72 However, the Team learnt that there was no specific instruction to specify the duration of leave in handling access rights of staff on leave. A staff from the ROP Division informed the Team that user un-assignment would normally be performed for lengthy annual leave or study leave. The un-assignment could be withheld if the staff was on *“a short duration of leave, say one to three weeks”*. These arrangements, however, were not mentioned in ImmD’s policies, guidelines or manuals.

- 5.73 **Response from ImmD:** Under the existing design of SMARTICS, the section head or officer-in-charge could perform transaction to assign or un-assign a user account in accordance with the guidelines as stipulated in Paragraph 9.2 of the IT Security Guidelines. But in practice, most user sections normally do not un-assign officers on short leave except those on lengthy one. Nevertheless, there is internal departmental instruction i.e. ISSO 9.1 stating that a staff will not return to his office/place of duty where he is not on duty and prior permission needs to be sought from the section head before he can return to the office during the leave period. Besides, the section head or officer-in-charge could monitor and identify any irregular logon from relevant audit trail reports. Taking into consideration of the Commissioner's finding, ImmD will consider to set out more specific guidelines on temporarily disabling access right of staff on leave.

Objective of the Recommendation 14

Written departmental procedure of temporarily disabling access by staff members who are on leave is to be followed.

RECOMMENDATION 14

1. To review the appropriateness of the departmental procedure on access for staff on leave taking into consideration of the operational need.
2. To impress upon staff members the importance of following the departmental guidelines on access control for staff who are on leave.
3. To consider the need to issue or enhance procedures to strengthen the compliance of such guidelines.

Audit Trails

- 5.74 This is a follow-on finding on the specific findings under the Policy Review about the lack of dedicated guidelines for users who need to carry out audit trail checks.

- 5.75 In the absence of detailed guidelines, the Team was unable to trace the audit trails of user access and account assignment/un-assignment effectively. The Team found that the audit trail reports were not user-friendly. It was noted that at least three audit trails reports, i.e. User Assignment Events Summary, User Un-assignment Events Summary and User Management Transaction Summary had to be reviewed simultaneously and manually with ImmD posting orders to check for any irregularity on user access and account assignment / un-assignment.
- 5.76 The Commissioner does not believe that it is feasible in practice to cross-examine all these bulky printouts regularly to detect irregularity in a consistent manner.
- 5.77 **Response from ImmD:** Guidelines on checking audit trail reports are available in SMARTICS Security Guidelines and SMARTICS Manual Procedures, Volume I Chapter 11.11, Volume II Chapter 4.1 and Volume III Chapter 7.1. With these guidelines, the mechanism of conducting checks on audit trails has been running effectively over the years. However, taking into consideration of the Commissioner's finding, more specific and consistent guidelines will be provided to section heads or officers-in-charge of user sections/offices to facilitate a more effective checking of audit logs for identifying irregularities. Training and awareness programs will also be arranged as required.

This need for having a more dedicated audit trail review guideline on how to conduct review was identified previously under Policy Review (Chapter 4). The finding here in the Workflow Review only reinforced the previous finding, that in the absence of a detailed guideline, it would not be easy for reviewers to identify inappropriate rights and unauthorised access effectively and consistently. The objective and recommendation of this specific finding repeat Recommendation 4.

Specific Findings that Need Improvements/Reviews

- 5.78 The specific findings in this section may not pose an immediate

impact when compared with those listed above. Nevertheless, these findings do have implication to the security of Smart ID Card Data and therefore should be addressed.

Access Control

- 5.79 ImmD self-service kiosks help individuals check their personal data stored in the Chips of their Smart ID Cards by using a card reader installed thereat. However, the kiosks will capture (withheld) a Smart ID Card and suspend the immigration on-card application if any of the following events occurs: (a) the date of registration of the card does not tally with that in the database; (b) there is a death indicator in respect of the card; (c) the status of the card has become invalid (e.g. invalidated identity card); or (d) the limit of stay of the card holder has expired.
- 5.80 ImmD had written procedures for staff to follow in handling card-capturing incidents. The Manual Procedures states that when a kiosk captures an inserted Smart ID Card, ImmD staff should retrieve the Smart ID Cards from the kiosk, interview the card holder in a meeting room and examine the card to find out the cause of the card capturing. Moreover, the staff should properly record the incident in a register.
- 5.81 The information of card capturing will be recorded in a batch computer report which will be dispatched to the relevant section by the SMARTICS Controller on the next working day. On receipt of the computer report, a Senior Immigration Officer of the section has to check against the control register to ensure all the cards captured have been properly handled and accounted for. The Senior Immigration Officer will sign on the computer report to confirm the checking. The Chief Immigration Officer of the respective section is required to conduct spot checks to ensure no irregularities and to enter the result in a spot check register.
- 5.82 During the assessment, the Team observed two card capturing cases at the ROP Fo Tan Office and ROP Kowloon Office in August 2009.

5.83 At ROP Fo Tan Office, the Team noted that an ImmD staff had appeared not to have made any written record nor interviewed the cardholder to check her identity and the authenticity of the card when handling the card capturing case. The card was simply returned to the cardholder after being retrieved from the kiosk. The capturing was recorded in the relevant computer report but there was no entry in the control register for the whole month of August 2009 to record the incident. Besides, the responsible checker had failed to discover the discrepancy between the control register and the computer report.

5.84 At ROP Kowloon Office, the Team noted that an ImmD staff had recorded the information of a captured Smart ID Card after retrieving it from a kiosk. He returned it to the cardholder without inviting him for an interview to ascertain his identity and check the reason for the card capturing despite the cardholder had inquired into it.

5.85 In both cases, the handling ImmD staff did not appear to have taken any practicable steps to ascertain the identity of the cardholders before releasing the captured identity cards to them, which amounted to a departure from the Manual Procedures.

5.86 **Response from ImmD:**

5.86.1 Staff of ROP Offices are well aware of the Manual Procedures and the need to verify the identity of the applicants no matter in the processing of applications or handling of card capturing cases at the self-service kiosks.

5.86.2 For the card capturing incident happened at ROP-KO, internal investigation revealed that the staff who handled the incident had actually checked the facial appearance of the cardholder against the card and confirmed that he was the rightful holder. Given that the cardholder was the genuine and rightful holder, the staff

returned the card to him after recording the incident in a register without inviting him to an interview room.

5.86.3 For the card-capturing incident occurred at FTO, record check revealed that the cardholder was a HK-born permanent identity card holder whose Smart ID card had never been reported lost or invalidated. The staff concerned was unable to recall the incident in view of long lapse of time, but confirmed that it was his normal practice to conduct a cursory checking of the holder's facial appearance against the ID card on the spot before returning the card to the cardholder. The staff was aware that normal verification process should go through the proper procedures by checking the details e.g. the photo, residential status, identity of the cardholder, and the authenticity of the questioned ID card etc. However, the staff had mistaken that only card capturing case with irregularity would be required for entering into the control register. As the incident on the material date bore no irregularity, the staff did not enter such incident in the control register. Card capturing cases are not commonly encountered at ROP Offices. Nevertheless, taking the incidents, ImmD will strengthen the briefings and coaching for the staff on the proper protocol in handling card capturing cases. All staff will be reminded to strictly adhere to the laid down procedures concerning the operation of the self-service kiosk as stipulated in the SMARTICS Manual Procedures. Regular circulation of the relevant Manual Procedures will be arranged to fortify the staff's awareness and compliance.

5.86.4 Taking into consideration of the Commissioner's finding, ImmD will strengthen the briefings and coaching to remind the staff to strictly adhere to the laid down procedures and the proper protocol in handling Smart ID Cards captured by the self-service kiosks.

Objective of the Recommendation 15

To ensure compliance with the established procedures in relation to the returning, logging and checking of Smart ID Cards captured by self-service kiosks.

RECOMMENDATION 15

1. To increase the ImmD staff's awareness of the importance of observing the protocols for handling Smart ID Cards captured by immigration self-service kiosks.
2. To increase the level of awareness of the senior staff officers of the ImmD the importance of the reconciliation checks on computer reports and control registers.

5.87 As mentioned in the Policy Review, paragraph 8.6.6 of the IT Security Policy states: *“Users shall change their passwords at least once every three months or whenever deemed necessary”* whereas paragraph 14.6 of the SMARTICS Security Guidelines does not follow this more authoritative policy and states a lesser requirement of: *“Passwords for SMARTICS users are valid for six months”*.

5.88 SMARTICS Controller confirmed that change for new passwords in SMARTICS is mandatory upon every six months period. Besides, user password history is set to one. This means only one immediate password cannot be re-used thus an old password can be reused after one year.

5.89 Although the SMARTICS Security Guidelines does not recommend reuse of recent passwords, recurring use of the one in the second last time is allowed by the system. In reality this means user only need to use and rotate two passwords when using SMARTICS. The use of the same password, or a very limited number of passwords, increases the possibility of password being compromised and hence unauthorized access.

5.90 **Response from ImmD:** Taking into consideration of the

Commissioner's finding (This Recommendation will be jointly considered and followed up with Recommendation 5), the relevant SMARTICS Security Guidelines will be amended to be in line with the IT Security Policy that “Users shall change their passwords at least once every three months or whenever deemed necessary.” For the change in SMARTICS to oblige users to change their passwords every three months, it would take some time to implement the change.

Objective of the Recommendation 16 (To be read in conjunction with Recommendation 5)

This recommendation should be read in conjunction with Recommendation 5. It addresses the same issue discovered during the Policy Review as well as an additional point revealed during the Workflow Review. It’s objective is to ensure that the minimum length of time requirement for password changes is uniform at departmental and system levels. To strengthen the frequency of password changes and history controls is to ensure that passwords in use do get changed regularly.

RECOMMENDATION 16

1. To align the SMARTICS guideline with the departmental guideline so that passwords are changed at least once every three months.
2. To consider strengthening the password history control of SMARTICS.
3. To configure SMARTICS to force password change with aligned expiry length of time and password history requirement, if appropriate.

DPP5 – Information to be Generally Available

General Comments

- 5.91 During the visits at the frontline ROP Offices and the Control Points at Lo Wu, Lok Ma Chau and the Airport, the Team observed that ImmD had made available the Statement of Purpose (the ImmD version of the PICS) for public access.

- 5.92 ImmD demonstrated its commitment and openness to personal data privacy protection by publishing the Privacy Policy in the form of a booklet and posters. The Privacy Policy and Statement of Purpose had been displayed at prominent places of the ROP Offices and the Control Points (Picture 6 in **Appendix VI**). The booklets would be provided to the public on request.
- 5.93 The above-mentioned practice allowed an individual to ascertain ImmD’s policies and practices in relation to personal data. It also served the purpose to inform the public about the kinds of personal data being held, and the main purposes for which personal data held by ImmD are or are to be used.
- 5.94 The Team further observed that ImmD had an established policy framework for privacy including the policies, guidelines, circulars and memos in relation to personal data protection. ImmD disseminated such documents by circulation (staff’s acknowledgement was required for specific circumstances where operation needs deem necessary) and briefing session held by staff’s supervisors. It was demonstrated by an ImmD officer that documents such as Department Circulars could be readily found from the Intranet portal.
- 5.95 The Commissioner was generally satisfied with the practicable steps taken by ImmD to make its policies and practices available to both public and its staff which is in line with the requirements of **DPP5**.

DPP6 – Access to Personal Data

General Comments

- 5.96 ImmD had issued a standing order ISSO requiring its staff to observe the requirements of the Ordinance in handling DAR and DCR. In addition, ImmD had designated the Records and Data Management Section to coordinate DAR requests for cross-divisional records. For cases involving cross-divisional records,

the Registration of Persons Division would assist to supply the relevant Smart ID Card Data to the applicant through the Records and Data Management Section which played the role of a coordinator. For mere request for Smart ID Card Data where only registration of persons records were involved, the request would be handled by the Registration of Persons Division. Between 1 July 2005 and 31 May 2009, ImmD received 626 DAR in relation to Smart ID Card Data. For compliance with the legal requirement, all requests received by ImmD were replied within the 40-day time limit. During the above-mentioned period, ImmD received no DCR in relation to Smart ID Card Data. No non-compliance cases were detected during the assessment period.

- 5.97 Furthermore, section 27 of the Ordinance requires a data user to keep a logbook to record all refusals of DAR and DCR and the particulars of the reasons for the refusals. To comply with the requirements of the Ordinance, ImmD kept and maintained such a logbook by respective sections. The Team examined the “Log Book on Refusal for Data Holding/Access/Correction Requests” maintained by Records & Data Management Section and Lo Wu Control Point. There was no record of refusal in relation to DAR/DCR requests on Smart ID Card Data.
- 5.98 Pursuant to section 28 of the Ordinance, a data user may impose a fee for complying with a DAR. The fee, if any, imposed for complying with such request shall not be excessive. Generally speaking, the Commissioner opines that the data user may be allowed to recover the labour costs and actual out-of-pocket expenses incurred for the location, retrieval and reproduction of the requested data involved in the process of complying with a DAR.
- 5.99 The Commissioner was generally satisfied with the degree of transparency of ImmD on informing the general public the rights to access their personal data, the way of accessing a DAR form, the way of requesting the correction of personal data and the fee for complying with DAR (i.e. at the current rate of \$1 per photocopy) which was explicitly specified in the Privacy Policy.

Conclusion

6.1 The SMARTICS launched by ImmD is a significant milestone achieved by the Government in providing Hong Kong people with an electronic smart card which contains personal identifiers for the purpose of legal identification of an individual. Having regard to the massive amount of sensitive personal data being handled and processed, the personal data protection measures adopted by ImmD to Hong Kong identity card holders have to be of a very high standard not only for the reason of compliance with the requirements of the Ordinance but also of meeting the legitimate privacy expectation of the public.

6.2 Since the SMARTICS has been in operation for some 7 years, it is appropriate and timely that a comprehensive review of its operation be conducted by way of an assessment of its level of compliance with the Ordinance. While PCA is a privacy audit tool which is usually performed by professional risk management or audit experts, the Commissioner accepted the invitation from the Government to perform the PCA because it is of great public interest to assess the privacy compliance level of SMARTICS from the regulator's perspective. In this audit, the Commissioner examined the personal data system of SMARTICS through policy and workflow review. Overall, the Commissioner found that the ImmD has appropriate policies, practices and guidance in place in handling and processing personal data system. There are some functional areas that require improvements and rectifications as mentioned in the recommendations given in this Report which highlight the need for ImmD :

- ◆ to improve its documentation review mechanism so that all policies and practices shall be clearly documented, updated, effectively communicated and executed by the staff in a consistent manner;
- ◆ to provide more frequent and regular on-the-job training to

the relevant staff to ensure their competence, ability and integrity in understanding and applying the Ordinance in their respective daily work performance; and

- ♦ to conduct systematic and regular reviews of the various operational aspects of the SMARTICS to ensure that the level of compliance is maintained in response to the changing environment, in particular, the impact brought by the rapid advancement in technology, changes in work procedures and personnel, etc.

6.3 The Commissioner wishes to stress the importance of the need for organizational data users like ImmD to build and maintain a privacy governance that incorporates a risk management approach that covers assessment, audit and breach management as the SMARTICS system develops over time.

6.4 The Commissioner has confidence that ImmD shall take all practicable steps to consider carefully and actively implement the recommendations made in this Report and will also promulgate a Code of Practice for approval by the Commissioner under section 12 of the Ordinance. Such Code of Practice will serve as a practical guide to facilitate compliance with the Ordinance by ImmD.

6.5 The Commissioner wishes to thank all members of the ImmD who have provided facilities, information and assistance to the Team in the carrying out of the PCA. The undertaking of this PCA and the publication of this Report shall not prejudice the exercise of the other regulatory functions and powers of the Commissioner under the Ordinance vis-à-vis the ImmD.



Roderick B WOO
Privacy Commissioner for Personal Data
30 July 2010

Glossary

Audit Trail	<i>Audit trail is a kind of record showing who has accessed a computer system and what operations he or she has performed during a given period of time.</i>
Biometric Verification	<i>Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits such as fingerprints.</i>
Data Protection Principles	<i>The data protection principles in Schedule 1 to the Personal Data (Privacy) Ordinance.</i>
Data Subject	<i>Data subject, in relation to personal data, means the individual who is the subject of the data.</i>
Data User	<i>Data user, in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.</i>
Encryption	<i>Encryption refers to algorithmic schemes that encode plain text into non-readable form or cyphertext, providing privacy. The receiver of the encrypted text uses a “key” to decrypt the message, returning it to its original plain text form.</i>
Need-to-know	<i>A method of isolating the information resources based on a user’s need to have access to that resources in order to perform their job but no more.</i>
Personal Data	<i>Section 2(1) of the Ordinance defines “personal data” to mean any data – (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.</i>
Practicable	<i>Section 2(1) of the Ordinance defines “practicable” to mean “reasonably practicable”.</i>

Privacy Impact Assessment	<i>Privacy Impact Assessment is a systematic risk assessment tool that can be usefully integrated into a decision-making process in evaluating a proposal in terms of its impact upon personal data privacy with the objective of avoiding or minimizing the adverse impact.</i>
Segregation Of Duties	<i>Segregation of duties means separating certain areas of responsibility and duties in an effort to reduce fraud and unintentional mistakes.</i>
Smart ID Card Data	<i>Means the items of information set out in Schedule 1 to the Registration of Persons Regulations that are personal data.</i>
The Ordinance	<i>Personal Data (Privacy) Ordinance, Cap. 486, Laws of Hong Kong.</i>

Appendix I - Personal Data (Privacy) Ordinance

Section 4 - Data protection principles

A data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under this Ordinance.

Schedule 1 – DATA PROTECTION PRINCIPLES

1. Principle 1 – purpose and manner of collection of personal data

- (1) Personal data shall not be collected unless-
 - (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
 - (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
 - (c) the data are adequate but not excessive in relation to that purpose.
- (2) Personal data shall be collected by means which are-
 - (a) lawful; and
 - (b) fair in the circumstances of the case.

- (3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that-
- (a) he is explicitly or implicitly informed, on or before collecting the data, of-
 - (i) whether it is obligatory or voluntary for him to supply the data; and
 - (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
 - (b) he is explicitly informed-
 - (i) on or before collecting the data, of-
 - (A) the purpose (in general or specific terms) for which the data are to be used; and
 - (B) the classes of persons to whom the data may be transferred; and
 - (ii) on or before first use of the data for the purpose for which they were collected, of-
 - (A) his rights to request access to and to request the correction of the data; and
 - (B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provision of data protection principle 6.

2. Principle 2 – accuracy and duration of retention of personal data

- (1) All practicable steps shall be taken to ensure that-
 - (a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;
 - (b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used-
 - (i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or
 - (ii) the data are erased;
 - (c) where it is practicable in all the circumstances of the case to know that-
 - (i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and
 - (ii) that data were inaccurate at the time of such disclosure, that the third party-
 - (A) is informed that the data are inaccurate; and
 - (B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.
- (2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. Principle 3 - use of personal data

Personal data shall not, without the prescribed consent of the data subject, be used for any purposes other than-

- (a) the purpose for which the data were to be used at the time of the collection of the data; or
- (b) a purpose directly related to the purpose referred to in paragraph (a).

4. Principle 4 – security of personal data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to-

- (a) the kind of data and the harm that could result if any of those things should occur;
- (b) the physical location where the data are stored;
- (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;
- (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
- (e) any measures taken for ensuring the secure transmission of the data.

5. Principle 5 - information to be generally available

All practicable steps shall be taken to ensure that a person can-

- (a) ascertain a data user's policies and practices in relation to personal data;
- (b) be informed of the kind of personal data held by a data user;
- (c) be informed of the main purposes for which personal data held by a data user are or are to be used.

6. Principle 6 – access to personal data

A data subject shall be entitled to-

- (a) ascertain whether a data user holds personal data of which he is the data subject;
- (b) request access to personal data-
 - (i) within a reasonable time;
 - (ii) at a fee, if any, that is not excessive;
 - (iii) in a reasonable manner; and
 - (iv) in a form that is intelligible;
- (c) be given reasons if a request referred to in paragraph (b) is refused;
- (d) object to a refusal referred to in paragraph (c);
- (e) request the correction of personal data;
- (f) be given reasons if a request referred to in paragraph (e) is refused; and
- (g) object to a refusal referred to in paragraph (f).

Appendix II – Documents reviewed during Policy Review

Policies

- Information Technology Security Policy for Immigration Department (August 2008)
- Statement of Privacy Policy and Practices

Guidelines

- Guidelines and Procedures On Information Security Incident Handling For Immigration Department (June 2003)
- Information Technology Security Guidelines for Immigration Department (Aug 2008)
- Information Technology Security Guidelines for SMARTICS (August 2008)
- Security Guidelines for Internet Users (June 2003)
- Security Guidelines for Standalone Computers (June 2003)

Procedures

- Manual Procedures (as at 8 June 2007)
- User assignment and un-assignment procedures

Ordinance and Regulations

- Registration of Persons Ordinance, Chapter 177
- Registration of Persons Regulations, Chapter 177 Subsidiary Legislation

Organizational Structure

- Organization Chart of ROP Sub-division
- Organization Chart of Systems Support (Identity Card and Travel Documents) Section
- Organization Chart of Systems Support (Security and Administrative Network) Section
- Organization Chart of SMARTICS Support Team under Technology Services Division
- Post, roles and responsibilities of officers/staff in relation to Smart Identity Card processing
- Responsibility of Immigration Officer in maintaining office security in the Verification Office
- Roles and responsibilities of offices in relation to Smart Identity Card Processing
- Role and Responsibility of SMARTICS Controllers

Standing Orders & Instructions

- Immigration Service Standing Orders 7.2
- Airport Division Standing Instruction No. 12/2006 – Enquiry and Disposal of Registration of Persons (ROP) Records
- Task Force Sectional Instruction No. 2/2003 – Portable Identity Card Readers (Handheld Readers)
- Investigation Sub-divisional Instruction No. 8/2003 re Portable Identity Card Reader (Handheld Readers)
- General Investigation Sectional Instruction No. 4/2003 re Portable Identity Card Readers (Handheld Readers)
- Outside Investigation Sectional Instruction No. 1/2003 re Portable Identity Card Readers (Handheld Readers)
- Special Investigation Sectional Instruction No. 2/2003 re Portable Identity Card Readers (Handheld Readers)

Workflows

- Workflow in relation to Smart Identity Card Processing
- Workflow of Handling Lost HK Identity Card Case at Lo Wo Control Point
- Workflow of Handling Lost HK Identity Card Case at Lok Ma Chau Control Point
- Workflow of Lost/Invalid/forged Hong Kong Identity Card case at Airport Control Point

Disaster Recovery Documents

- Disaster Recovery Operations Manual for Immigration Department dated 20 March 2009
- Disaster Recovery Plan for Immigration Department dated 20 March 2009
- Extracts of Computer Operation Procedures Manual and Database Operation Manual – Version 1.0 (November 2009)
- LTO Offsite List
- Report on Disaster Recovery Drill for Immigration Department 2007/2008 dated 30 June 2008
- Report on Disaster Recovery Drill for Immigration Department 2008/2009 dated 20 March 2009
- SMARTICS TSM Monthly Backup Summary Report for 2009
- Tape in and out records for SMARTICS
- TSM Check-out Tape Report and TSM Scratch Tape Report

Training Materials

- Brief on Fingerprint Identification Principles (for new staff to Verification Office)
- Training Materials for IO IA Induction Course
- Training Materials for SIA Efficiency Course

Contracts

- Blank contract for Cleaning Services
- Blank contract for Transport Services
- Extract of SMARTICS contract in relation to confidentiality requirements

Non-disclosure agreements

- Declaration on Leaving Government Service
- Joining Declaration – Official Secrets Ordinance (Cap. 521)
- Non-disclosure agreement of employees

Undertakings

- Confirmation by Staff of Immigration Department
- Deed of undertaking for handling of government information
- Undertaking for Handling of Government Information of Immigration Department

Security Matrices

- Security Matrix of Verification Office
- Security Matrix of Immigration Telephone Enquiry Unit
- Security Matrix of Confidential Records Unit
- Security Matrix of Record Provision Unit
- Security Matrix of Record Maintenance Unit
- Security Matrix of Records Office
- Security Matrix of ROP Record Section
- Security Matrix of Investigation Sub-Division
- Security Matrix of Control Points
- Security Matrix of ROP Offices and ROP(S) Section

Privacy Assessment Checklists

- 1st Self-assessment Exercise – Privacy Assessment Checklist for ROP Data
- 2nd Self-assessment Exercise – Privacy Assessment Checklist for ROP Data

Immigration Department Circulars (IDCs)

- IDC No. 44/96 re Compliance with Personal Data (Privacy) Ordinance
- IDC No. 45/96 re Personal Data (Privacy) Ordinance
- IDC No. 3/97 re Personal Data (Privacy) Ordinance
- IDC No. 7/97 re Guidance Notes on Compliance with Personal Data (Privacy) Ordinance
- IDC No. 28/97 re Imposition of Fees for Complying with Data Access Requests Under Section 28 of the Personal Data (Privacy) Ordinance
- IDC No. 45/99 re Contacts with the Office of the Privacy Commissioner for Personal Data (PCO)
- IDC No. 18/2001 re Unauthorised Disclosure of Official Information
- IDC No. 13/2002 re Official Secret Policy
- IDC No. 26/2007 re Security of Official Documents and Information
- IDC No. 6/2008 re Security in Handling of Departmental Information in the Internet and Departmental Intranet Portal
- IDC No. 7/2008 re Handling of Official Information on Removable Storage Media
- IDC No. 9/2008 re Compliance with Data Protection Principle 4 of Personal Data (Privacy) Ordinance
- IDC No. 2/2009 re Security in the Handling of Classified Documents
- IDC No. 6/2009 re Departmental Security Instructions

Immigration Department Notices (IDNs)

- IDN No. 229/96 re Reference Materials on Personal Data (Privacy) Ordinance and Code on Access to Information
- IDN No. 28/97 re Office of the Privacy Commissioner for Personal Data
- IDN No. 262/97 re Personal Data (Privacy) Ordinance
- IDN No. 282/97 re Personal Data (Privacy) Ordinance - Matching Procedure
- IDN No. 345/97 re Code on Access to Information
- IDN No. 14/98 re Code of Practice on the Identity Card Number and Other Personal Identifier
- IDN No. 319/98 re Personal Data (Privacy) Ordinance
- IDN No. 213/99 re Compliance with Data Access Request
- IDN No. 338/99 re Compliance with Personal Data (Privacy) Ordinance - Data Access Request Form

Circular Memorandum

- Circular Memorandum dated 8 May 2008 re Information Security Guidelines for Portable Electronic Storage Devices

Memos

- Memo dated 3 July 2006 re Disclosure of ROP Particulars under Section 11 of Registration of Persons Ordinance (Cap. 177)
- Memo dated 28 September 2006 re Access to ROP Data by Immigration Assistants of the Travel Document Sections and Branch Offices
- Memo dated 7 February 2007 re Access to ROP Data by Photographer I and II of the Travel Documents Sections
- Memo dated 29 May 2007 re Disclosure of Registration of Persons (ROP) Particulars under Section 11 of ROP Ordinance, Cap.177 – Plain Copy of ROP Records
- Memo dated 2 May 2008 re OGCI Circular No. 1/2008 – Protection of Information System and Data
- Memo dated 28 November 2008 re OGCI Circular No. 7/2008 – Revised Government IT Security Policy and Guidelines and Guiding Principles on the Use of Internet Services

eMemos

- eMemo dated 26 March 2008 re Amended Data Access Request Form and New Arrangement in Coordination of Data Access Request for Cross-divisional Records
- eMemo dated 20 June 2008 re Compliance with the Personal Data (Privacy) Ordinance
- eMemo dated 4 March 2009 re Protection of Official Information
- eMemo dated 3 April 2009 re Compliance with Data Protection Principle 4 of Personal Data (Privacy) Ordinance
- eMemo dated 11 May 2009 re Security and Proper Handling of Personal Data held in Information Systems
- eMemo dated 7 July 2009 re Compliance with Data Protection Principle 4 of Personal Data (Privacy) Ordinance
- eMemo dated 21 July 2009 re Compliance with the Personal Data (Privacy) Ordinance
- eMemo dated 10 September 2009 re Security and Proper Handling of Personal Data held in Information Systems

eMails

- eMail dated 8 June 2009 re Retention Period of Computer Printouts in Card Personalization
- email dated 19 June 2008 to re Reminder for conducting Daily Checking of Reports
- email dated 9 June 2009 re Re-circulation of Review of Access Rights under SMARTICS

Minutes

- Minutes on Retention Period for SMARTICS-related Reports Generated from Card Production System and Card Inventory System

Reports

IT Security Audit Reports

- Security Audit on the IT Security Control and Management Infrastructure for the Mission Critical Network of Immigration Department (Version 1.1) – December 2005
- Recommendation on the IT Security Control and Management Infrastructure for the Mission Critical Network of Immigration Department (Version 1.1) – October 2005
- Security Risk Assessment & Audit Services for the EXPRESS and SMARTICS of Immigration Department (Version 1.1) – February 2007
- IT Security Audit Report for the SMARTICS of Immigration Department (Version 1.0) – January 2009

Reports in relation to Self-service Kiosk

- Self-service Kiosk – Exception Report (Daily) for ROP Hong Kong Office (10 August 2009 to 10 September 2009)
- Self-service Kiosk – Exception Report (Daily) for ROP Kowloon Office (10 August 2009 to 10 September 2009)
- Self-service Kiosk – Exception Report (Daily) for ROP Kwun Tong Office (10 August 2009 to 10 September 2009)
- Self-service Kiosk – Exception Report (Daily) for ROP Fo Tan Office (10 August 2009 to 10 September 2009)
- Self-service Kiosk – Exception Report (Daily) for ROP Yuen Long Office (10 August 2009 to 10 September 2009)

Audit Trail Reports

Verification Office:

- CM001 – System Access Summary
- CM002 – Authentication Failure Summary
- CM006 – User Management Transaction Summary
- CM007 – Update Summary on User Maintenance Details
- CM015 – User Assignment Events Summary
- CM016 – User Unassignment Events Summary
- SC/R0075RE01 – Audit Trail Report on ROP Enquiry

Confidential Records Unit:

- SC/R0075RE01 – Audit Trail Report on ROP Enquiry

Others:

- Audit trail reports of AIM Section (May 2009)
- Audit trail reports of Task Force (May 2009)

Other Reports

- Posting orders, CM007 Update Summary on User Maintenance Details, CM015 User Assignment Events Summary and CM016 User Unassignment Events Summary of Lo Wu Control Point (April 2009)
- Posting orders, CM007 Update Summary on User Maintenance Details, CM015 User Assignment Events Summary and CM016 User Unassignment Events Summary of Airport Control Point (June 2009)
- Maintenance Services Reports for (i) Uninterruptible Power Supply; (ii) Air-conditioning; (iii) Security; and (iv) Fire engineering maintenance
- Preventive Maintenance Reports of 18/F Immigration Tower (October 2008 to September 2009)
- Preventive Maintenance Reports of Resilience Centre (October 2008 to September 2009)
- Preventive Maintenance Reports of Lo Wu Control Point (October 2008 to September 2009)
- Preventive Maintenance Reports of Lok Ma Chau Control Point (October 2008 to September 2009)
- Performance Report on Maintenance Services for Production Systems provided by IT Services Provider of SMARTICS
- Preliminary report on the findings and recommendations of the 2nd Privacy Compliance Self-assessment Exercise

- Report SC/ASCRP02 – Monthly Workload Statistics Report (Confidential Records Unit)
- Report SC/ASCRP10 – Statistics on Disclosure of ROP Records for Requests from Public Authorities and other organization of Confidential Records Unit

Registers

Spot Check Registers

Verification Office:

- Spot Check Register on High Score Cases in Verification Pending Spot Check Queue
- Spot Check Register on Low Score Cases in Verified Pending Queue
- Spot Check Register in First Register Queue
- COMS Report Check Register

Others:

- Spot Check Register for ROP Records Office
- Spot Check Register for Confidential Records Unit
- Spot Check Register of AIM Section (May 2009)
- Spot Check Register of Task Force (May 2009)
- Spot Check Register for card dispatch of ROP Hong Kong Office (10 August 2009 to 10 September 2009)
- Spot Check Register for card dispatch of ROP Kowloon Office (10 August 2009 to 10 September 2009)
- Spot Check Register for card dispatch of ROP Yuen Long Office (10 August 2009 to 10 September 2009)
- Spot Check Register of ROP Hong Kong Office (IC Application)
- Spot Check Register of ROP Kowloon Office (Computer Reports)
- Spot Check Register of ROP Kwun Tong Office (Card Dispatch)
- Spot Check Register of ROP Yuen Long Office (All ROP Registers)
- Spot Check Register of Immigration Telephone Enquiry Unit (March to September 2009)

Other Registers

- Control Register for ID Card captured by Self-service Kiosk – ROP Kowloon Office
- Register for I/C Captured by the Smartic Kiosk – ROP Fo Tan Office
- Register On Suspected Impersonation Cases
- Register for Cases Routed Back from Verification Office to Front Offices
- Regular Review of User Access Rights under the SMARTICS – Verification Office
- ROP enquiry registers of AIM Section (May 2009)
- ROP enquiry registers of Task Force (May 2009)
- Register on the Allocation of SMARTICS Access Rights to Section Heads/Branch Officer-in-Charge managed by SS(SA) Section

Log Book

- Log Book on Refusal for Data Holding/Access/Correction Requests

Forms

- Form COS/ICTR/11 - Media Request Form
- Form PCRf - Production Change Request Form
- Form ROP1 – Application for a Permanent Identity Card/an Identity Card by a person of the age of 18 years or over
- Form ROP2 – Application for a Permanent Identity Card /an Identity Card by a person from the age of 11 years to 17 years
- Form ROP3 – Application for a Permanent Identity Card by a person under the age of 11 years
- Form ROP143 – Application for a Hong Kong Permanent Identity Card by a Person of the Age of 18 years or over Resident Overseas
- Form ROP144 – Application for a Hong Kong Permanent Identity Card by a person under the age of 18 Resident Overseas
- Form ROP73 – Application for Amendment of Registered Particulars of Hong Kong Identity Card
- Form ROP99 – Memo for Identity Card Record Check
- Form SF/ROP/91 – ITEU Request for Information

Document Control

- Document Control for Verification Office
- Document control for SS(IT) Section

Documents related to Automated Vehicle Clearance (AVC) System

- Enrolment Form of AVC System
- Operation Flow of AVC System
- Statement of Purpose of AVC System

Documents related to Automated Passenger Clearance System (Express e-Channel)

- Enrolment Form of Express e-Channel
- Express e-Channel poster
- Express e-Channel leaflet
- Flow of enrolment of Express e-Channel Service

LegCo papers

- “Panel on Security of the Legislative Council HKSAR Identity Card Project – Initial Privacy Impact Assessment Report” dated 6 February 2001 with “Initial Privacy Impact Assessment Summary of Recommendations”
- “Panel on Security of the Legislative Council HKSAR Identity Card Project – Latest developments and the Second Privacy Impact Assessment Report” dated 4 July 2002 with “Second Privacy Impact Assessment Summary of Recommendations”
- “Panel on Security of the Legislative Council HKSAR Identity Card Project: Progress Report” dated 6 January 2004 with “Third Privacy Impact Assessment Summary of Recommendations”
- “Panel on Security of the Legislative Council HKSAR Identity Card Project: Progress Report” dated 14 February 2005 with “Fourth Privacy Impact Assessment Summary of Recommendations”

IT Security Policies for Government bureaux/departments

- Regulations of the Government of the Hong Kong Special Administrative Region, Volume 5, Security Regulations (1998)
- Technical Notes Pursuant to Chapter XI of the Security Regulations (July 2007)

Others

- Daily Workload Statistics for Verification Office
- Document on the security features of Secure Access Module (SAMs)
- Extracts of ICAC Assignment Report No. 96/2003
- Extracts of memo of 1 June 2004 from Director of Immigration to Director of Corruption Prevention in response to the ICAC Assignment Report No. 96/2003
- General and Departmental Common Grades Posting Notice No.: 4/2009
- Immigration Telephone Enquiry Unit Daily Statistics Report as at 11 August 2009
- List of computer reports available for checking by SIOs or their delegates
- Monthly Statistics on Requests for ROP records handled by RPU (Mar 2009-Sep 2009)
- Office Daily Handling Capacity (ROP/Joint Offices)
- Retention Period of Files / Records in ROP Division containing ROP data (Version as at July 2009)
- Screen dump of Intranet Portal
- Screen dump of SMARTICS
- Ten Dos and Ten DON'Ts to help protect your computers from cyber attacks
- User manual for changing the content of Transaction Group / template in SMARTICS

Appendix III - Offices visited

Registration of Persons Offices

- Registration of Persons – Hong Kong Office
- Registration of Persons – Kowloon Office
- Registration of Persons – Kwun Tong Office
- Immigration and Registration of Persons – Fo Tan Office
- Immigration and Registration of Persons – Yuen Long Office

Immigration Control Points

- Hong Kong International Airport
- Lo Wu
- Lok Ma Chau

Registration of Persons (Records) Section

- Card Personalisation Office
- Confidential Records Unit
- Operations Support Office
- Records Office
- Verification Office

Other ImmD Offices

- Anti-illegal Migration Agency
- Investigation Sub-division
- System Section (SMARTICS Controller)
- Disaster Recovery Centre
- Resilience Centre
- Offsite backup centre

Appendix IV - Questionnaire for identity card applicants

(A) Questionnaire



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Questionnaire for identity card applicants 問卷

Date: 12th August 2009 to 18th August 2009

日期：二零零九年八月十二日至十八日

Please answer this questionnaire in English.

(The English version is the original. The Chinese version is a translation of it)

請填寫本問卷之英文版

(本問卷以英文撰寫，中文為翻譯本)

For PCPD staff only

此欄只供公署人員使用

Begin at:

開始時間 _____

End at:

結束時間 _____

Name and signature of PCPD staff:

公署人員姓名及簽署

1. What was the purpose of your visit to ROP Office today?
 - a. Applying for an identity card (for the age of 18 years or above)
 - b. Applying for an identity card (from the age of 11 years to 17 years)
 - c. Applying for replacement of an identity card due to loss, defacement or destruction
 - d. Applying for replacement of an identity card due to amendment

2. Do you understand the content of the “Statement of Purpose” printed on the application form?
 - a. Yes
 - b. Not sure
 - c. I am not aware of any Statement of Purpose

3. Did the handling staff explain the content of the “Statement of Purpose” to you?
 - a. Yes, the staff explained voluntarily
 - b. Yes, the staff explained as per my request
 - c. No

4. Did the handling staff explain the consequences of not providing the requested information in the application form?
 - a. Yes, the staff explained voluntarily
 - b. Yes, the staff explained as per my request
 - c. No

5. Did the handling staff use his/her mobile phone or other portable electronic device (e.g. PDA) when processing your application?
 - a. Yes
 - b. No

6. Do you agree that the Immigration Department had provided an environment with sufficient privacy to process your application?
 - a. Yes
 - b. No, please give details _____
 - c. No comment

7. Did you use the Self Service Kiosk?
 - a. Yes
 - b. No (go to Q9)

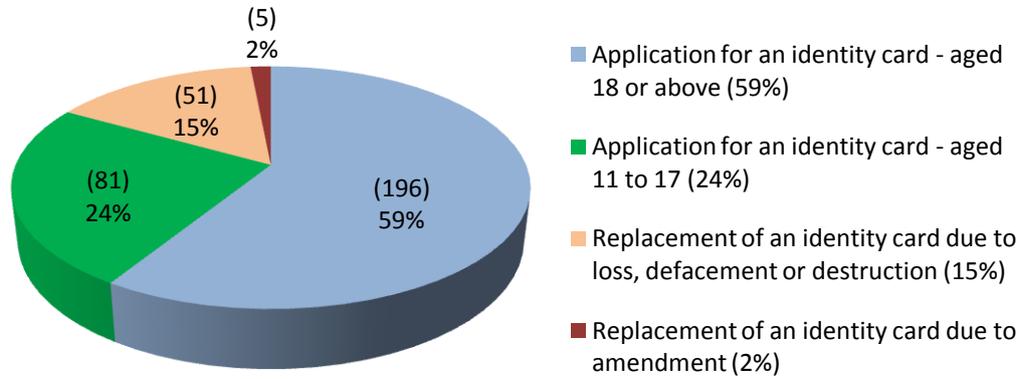
8. Do you consider that your personal data were well protected when using the Self Service Kiosk?
 - a. Yes
 - b. No, please give details _____
 - c. No comment

9. Do you consider that your personal data were well protected when the handling staff processed your application?
- a. Yes
 - b. No, please give details _____
 - c. No comment

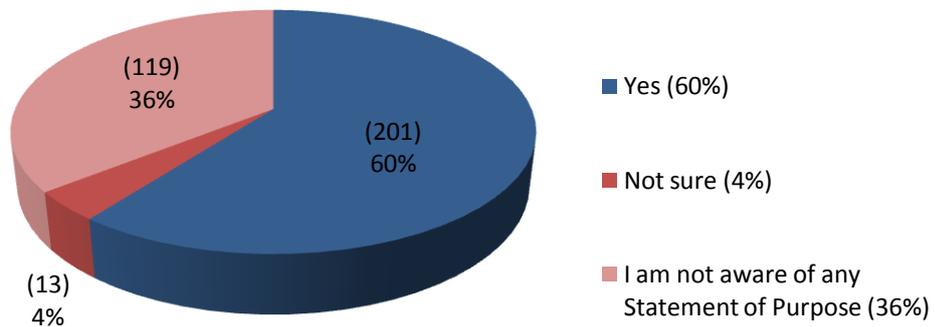
- End -

(B) Results analysis

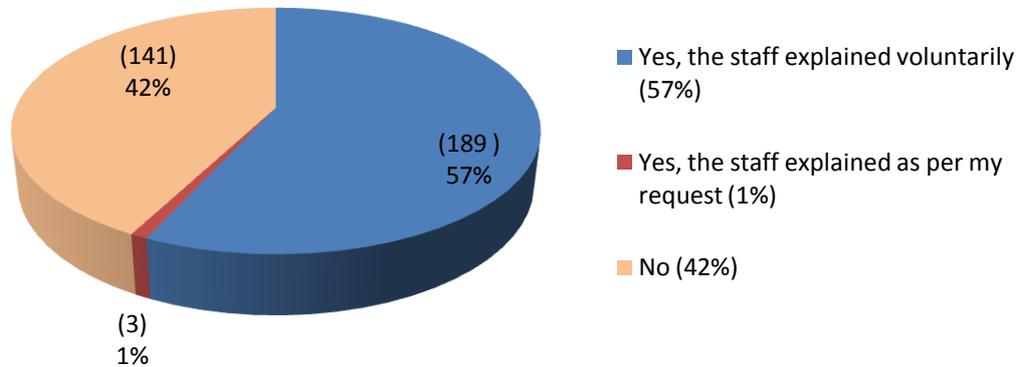
1. What was the purpose of your visit to ROP Office today?



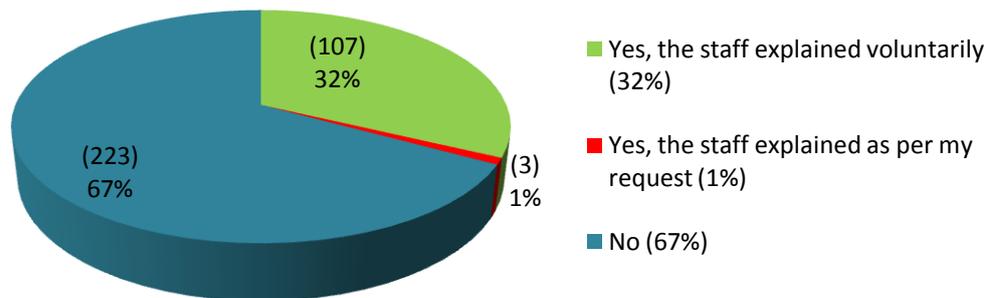
2. Do you understand the content of the “Statement of Purpose” printed on the application form?



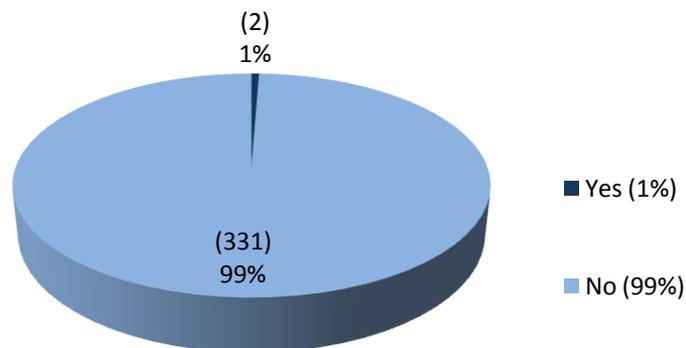
3. Did the handling staff explain the content of the “Statement of Purpose” to you?



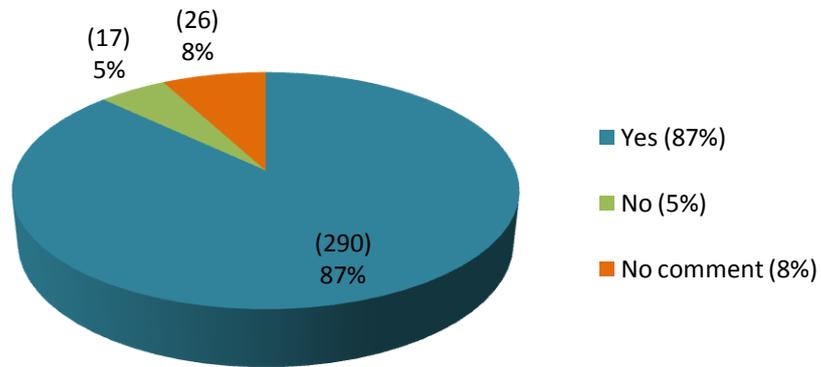
4. Did the handling staff explain the consequences of not providing the requested information in the application form?



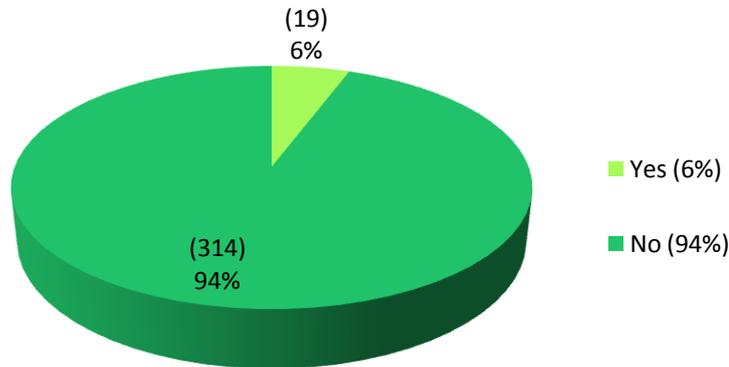
5. Did the handling staff use his/her mobile phone or other portable electronic device (e.g. PDA) when processing your application?



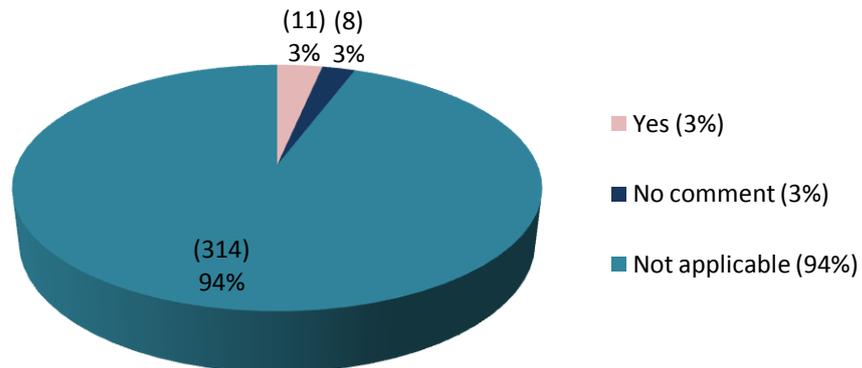
6. Do you agree that the Immigration Department had provided an environment with sufficient privacy to process your application?



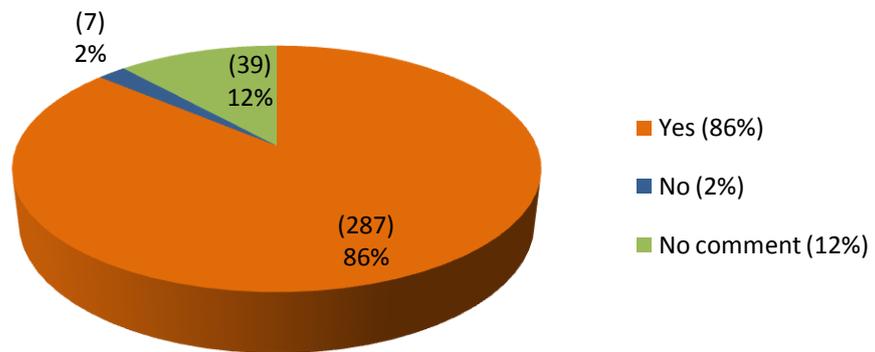
7. Did you use the Self Service Kiosk?



8. Do you consider that your personal data were well protected when using the Self Service Kiosk?



9. Do you consider that your personal data were well protected when the handling staff processed your application?



Remarks:

- (1) There are altogether 333 submissions and all are valid*
- (2) All figures are rounded off*

Appendix V - Questionnaire for staff of Immigration Department

(A) Questionnaire



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Questionnaire 問卷

Date: 4th November 2009

日期：二零零九年十一月四日

Please answer this questionnaire in English.

(The English version is the original. The Chinese version is a translation of it)

請填寫本問卷之英文版

(本問卷以英文撰寫，中文為翻譯本)

For PCPD staff only

此欄只供公署人員使用

Begin at:

開始時間_____

End at:

結束時間_____

Name and signature of PCPD staff:

公署人員姓名及簽署

This Questionnaire forms part of a privacy compliance audit carried out by the Privacy Commissioner for Personal Data on Smart Identity Card System (“SMARTICS”) of the Immigration Department (“ImmD”) to assess and evaluate whether ImmD has effectively complied with the requirements of the Personal Data (Privacy) Ordinance in relation to the handling of Smart Identity Card Data.

“Smart Identity Card Data” means any item of information set out in Schedule 1 to the Registration of Persons Regulations, which stipulates that :

“1. Every identity card shall include-

- (a) the full personal name and surname of the applicant in English or in English and Chinese;*
- (b) the Chinese commercial code (if applicable);*
- (c) the date of birth of the applicant;*
- (d) a number for identification purposes;*
- (e) the date of issue of the card;*
- (f) a photograph of the applicant, unless the applicant is under the age of 11 years; (9 of 2003 s.20)*
- (g) such data, symbols, letters or numbers representing prescribed information, particulars or data within the meaning of section 7(2A)(b) of the Ordinance as the Commissioner may determine; and (9 of 2003 s.20)*
- (h) in the form of data stored in the chip in the identity card-*
 - (i) template of the applicant’s thumb-prints or other fingerprints taken under regulation 4(1)(a);and*
 - (ii) (where the applicant does not have a right of abode in Hong Kong) the conditions of stay (including a limit of stay) imposed in relation to him under section 11 of the Immigration Ordinance (Cap 115). (9 of 2003 s.20)...”*

For the purposes of this Questionnaire, “access” means and includes the coming into contact with (including the collection, processing and disposal of) Smart Identity Card Data whether in paper or electronic form.

You are not asked to disclose your identity in completing this questionnaire nor will any identifiable data in the completed questionnaire be passed to ImmD. Please read the following questions carefully before giving your answers by either ticking the boxes or filling in the blanks. Your assistance is appreciated.

本問卷屬個人資料私隱專員對入境事務處(下稱「入境處」)的智能身份證系統進行私隱循規審核的一部分，以評估入境處在處理智能身份證資料方面是否有效地依從《個人資料(私隱)條例》的規定。

「智能身份證資料」指《人事登記規例》附表 1 所列的任何資料，該規例訂明：

「1. 每張身分證須包括—

- (a) 申請人姓氏及個人名字的英文或中英文全寫；
- (b) 中文字的商用電碼(如適用的話)；
- (c) 申請人的出生日期；
- (d) 作識別用途的編號；
- (e) 該證的發出日期；
- (f) 申請人照片(申請人不足 11 歲者除外)；(2003 年第 9 號第 20 條)
- (g) 處長決定的代表本條例第 7(2A)(b)條所指的訂明資料、詳情或數據的數據、符號、英文字母或號碼；及 (2003 年第 9 號第 20 條)
- (h) 以數據形式儲存於身分證內的晶片內的—
 - (i) 根據第 4(1)(a)條套取的申請人的拇指指紋或其他手指的指紋的模版；
及
 - (ii) (凡申請人沒有香港居留權)根據《入境條例》(第 115 章)第 11 條就申請人施加的逗留條件(包括逗留期限)。 (2003 年第 9 號第 20 條)...

就本問卷而言，「查閱」的意思包括與智能身份證資料(不論是紙張形式或電子形式)的接觸(包括收集、處理及棄置)。

你在填寫本問卷時無需披露你的身份，本署亦不會向入境處披露問卷中可以核實你身份的資料。請詳閱各問題，然後以✓號選擇你的答案，或在空白處填上你的答案。謝謝你的協助。

1. **Your present job type is:**
 - A. Registration Officer
 - B. Clerical staff
 - C. Administrative/managerial staff
 - D. Others, please specify: _____

2. **Which category of staff do you belong to:**
 - A. Disciplined service grades
 - B. General and common grades
 - C. Non-civil Services Contract staff
 - D. Others, please specify: _____

3. **How long have you been working in ImmD?**
 - A. Less than 1 year
 - B. 1 year to less than 3 years
 - C. 3 years to less than 5 years
 - D. 5 years to less than 8 years
 - E. 8 years or above

4. **How long have you been working in your current section?**
 - A. Less than 1 year
 - B. 1 year to less than 3 years
 - C. 3 years to less than 5 years
 - D. 5 years to less than 8 years
 - E. 8 years or above

5. **In the discharge of your job duties, what form of Smart Identity Card Data will you handle?**
 - A. Paper form
 - B. Electronic form
 - C. Both A and B

6. **Were you required to sign an undertaking that you would comply with the SMARTICS security requirements when you received the user ID and password?**
 - A. Yes
 - B. No
 - C. I don't remember
 - D. I was not required to sign an undertaking because I was not given the access right to SMARTICS. (Please go to Question 11 directly)

7. **Are your access rights to SMARTICS commensurate with your job responsibilities?**
 - A. Yes
 - B. No

If yes, do you find your access rights to SMARTICS sufficient for performing your duties?

- i. Yes, it is more than sufficient
- ii. Yes, it is sufficient
- iii. No, it is not sufficient

1. 你現時的工作類別是：
 - A. 登記主任
 - B. 文書人員
 - C. 行政/管理人員
 - D. 其他，請註明：_____

2. 你屬於甚麼職系的人員？
 - A. 紀律部隊職系
 - B. 一般和共通職系
 - C. 非公務員合約人員
 - D. 其他，請註明：_____

3. 你在入境處工作多久？
 - A. 1 年以下
 - B. 1 年至 3 年以下
 - C. 3 年至 5 年以下
 - D. 5 年至 8 年以下
 - E. 8 年或以上

4. 你在現時的部門工作多久？
 - A. 1 年以下
 - B. 1 年至 3 年以下
 - C. 3 年至 5 年以下
 - D. 5 年至 8 年以下
 - E. 8 年或以上

5. 你在履行職責時，所處理的智能身份證資料是甚麼形式？
 - A. 紙張形式
 - B. 電子形式
 - C. 以上兩者都有

6. 當你收到用戶名稱及密碼時，是否需要簽署承諾書，承諾你會遵守智能身份證系統的保安規定？
 - A. 需要
 - B. 不需要
 - C. 不記得
 - D. 我不需要簽署承諾書，因為我沒有查閱智能身份證系統的權限。(請轉往第 11 題)

7. 你查閱智能身份證系統的權限是否與你的職責相稱？
 - A. 是
 - B. 不是

如是，你查閱智能身份證系統的權限是否足夠讓你履行職責？

 - i. 足夠有餘
 - ii. 足夠
 - iii. 不足夠

8. Have you ever changed your password for SMARTICS before the system prompts you to do so?

- A. Yes
- B. No
- C. I do not remember

9. Do you log out SMARTICS whenever you leave your terminal?

- A. Always
- B. Sometimes
- C. Never, I rely on auto log-out mechanism

10. Do you know that all of your transactions performed in SMARTICS are logged by the system?

- A. Yes
- B. No

If yes, according to the retention policy of ImmD, how long will the hard copies of audit trail reports be retained?

- i. 6 months
- ii. 2 years
- iii. 7 years
- iv. Permanent
- v. I do not know

11. Have you ever read the following ordinance, policies, guidelines or practices of ImmD? (You may choose to tick more than one box)

- A. Section 17 of the Official Secrets Ordinance
- B. Information Technology Security Policy for Immigration Department
- C. Information Technology Security Guidelines for Smart Identity Card System
- D. Immigration Department Circular No. 9/2008 – Compliance with Data Protection Principle 4 of Personal Data (Privacy) Ordinance
- E. Immigration Department Circular No. 2/2009 – Security in the Handling of Classified Documents
- F. No, I am not aware of any of the above

If yes, how do you know of their existence? (You may choose to tick more than one box)

- i. During formal training
- ii. Being informed by my supervisor, either verbally or in writing
- iii. Finding them out myself from the intranet
- iv. Others, please specify: _____

12. Does your supervisor follow the guidelines of ImmD to store away hard copies of Smart Identity Card Data when not in use?

- A. Yes
- B. No

13. Does your supervisor regularly inspect if there is any hard copy of Smart Identity Card Data is retained longer than the period specified in the retention policy of ImmD?

- A. Yes
- B. No
- C. I do not know

8. 你有沒有在智能身份證系統催促你更改密碼之前，自行更改你的密碼？
- A. 有
B. 沒有
C. 不記得
9. 你在離開終端機之前，有否登出智能身份證系統？
- A. 經常
B. 有時
C. 從不，我是依賴系統自動登出的
10. 你是否知道你在智能身份證系統中所作的所有事項均會由系統記錄下來？
- A. 知道
B. 不知道
- 如知道，根據入境處的文件保留政策，審計追蹤的文本會保留多久？
- i. 6 個月
ii. 2 年
iii. 7 年
iv. 永久
v. 不知道
11. 你會否閱覽過以下條例、政策、指引或措施？(可選擇多於一項)
- A. Section 17 of the Official Secrets Ordinance (官方機密條例第 17 條)
B. Information Technology Security Policy for Immigration Department
C. Information Technology Security Guidelines for Smart Identity Card System
D. Immigration Department Circular No. 9/2008 – Compliance with Data Protection Principle 4 of Personal Data (Privacy) Ordinance
E. Immigration Department Circular No. 2/2009 – Security in the Handling of Classified Documents
F. 以上所述，我全不知道
- 如有，你是如何得知上述條例、政策、指引或措施？(可選擇多於一項)
- i. 在正式培訓期間
ii. 我的上司口頭或書面通知我
iii. 我自行在內聯網上找到
iv. 其他，請註明：_____
12. 你的上司會否跟從入境處的指引，儲存使用中的智能身份證資料文本？
- A. 會
B. 不會
13. 你的上司會否定期檢查所保留的智能身份證資料文本有沒有依從入境處文件保留政策所指定的保留期限？
- A. 會
B. 不會
C. 不知道

**14. Which of the following is/are official classification(s) of Smart Identity Card Data?
(You may choose to tick more than one box)**

- A. Top Secret
- B. Secret
- C. Confidential
- D. Restricted
- E. General

15. Have you attended a training session in personal data privacy protection?

- A. Yes
- B. No

If yes, when did you receive the last training?

- i. Less than 1 year ago
- ii. 1 year to less than 3 years ago
- iii. 3 years to less than 5 years ago
- iv. 5 years ago or above

If yes, did you find the training helpful in addressing the security of Smart Identity Card Data?

- (a) Helpful
- (b) Not helpful
- (c) I don't know

16. If a staff member reports to his supervisor that an application form ROP1 containing Smart Identity Card Data that was registered on 1 September 2008 and had not been disposed is missing, which of the following Data Protection Principle(s) of the Personal Data (Privacy) Ordinance might be involved? (You may choose to tick more than one box)

- A. Principle 1 – purpose and manner of collection of personal data
- B. Principle 2 – accuracy and duration of retention of personal data
- C. Principle 3 – use of personal data
- D. Principle 4 – security of personal data
- E. Principle 5 – information to be generally available
- F. Principle 6 – access to personal data
- G. None of the above
- H. I do not know

17. How do you rate the overall measures adopted by ImmD to protect the security of Smart Identity Card Data?

- A. Very sufficient
- B. Sufficient
- C. Insufficient
- D. Very insufficient

18. How do you rate your colleagues' level of observance of the requirements of ImmD in safeguarding the security of Smart Identity Card Data?

- A. Fully observed
- B. Broadly observed
- C. Partially observed
- D. Not observed

14. 下述哪項是智能身份證資料的官方分類？(可選擇多於一項)

- A. 絕對機密
- B. 高度機密
- C. 機密
- D. 限閱文件
- E. 一般文件

15. 你有沒有參加過有關保障個人資料私隱的培訓？

- A. 有
- B. 沒有

如有，最近一次培訓是在何時？

- i. 1年內
- ii. 1年至3年以下
- iii. 3年至5年以下
- iv. 5年或以上

如有，你認為該次培訓對應付智能身份證資料的保障是否有幫助？

- (a) 有幫助
- (b) 沒有幫助
- (c) 不知道

16. 如有人員向其上司報告遺失一份載有智能身份證資料的 ROP1 申請表，該表是於 2008 年 9 月 1 日登記，但未被棄置，這可能會涉及《個人資料(私隱)條例》哪項保障資料原則？(可選擇多於一項)

- A. 第 1 原則 – 收集個人資料的目的及方式
- B. 第 2 原則 – 個人資料的準確性及保留期間
- C. 第 3 原則 – 個人資料的使用
- D. 第 4 原則 – 個人資料的保安
- E. 第 5 原則 – 資訊須在一般情況下可提供
- F. 第 6 原則 – 查閱個人資料
- G. 以上全都不是
- H. 不知道

17. 你如何評價入境處在保障智能身份證資料方面的整體措施？

- A. 非常充足
- B. 充足
- C. 不足
- D. 非常不足

18. 你如何評價你的同事在遵守入境處的保障智能身份證資料規定的程度？

- A. 完全遵守
- B. 廣泛遵守
- C. 部分遵守
- D. 不遵守

19. Have you ever seen any sharing of SMARTICS log-in passwords with others in your section?

- A. Yes
- B. No

20. Have you ever seen any SMARTICS terminal not logged out after use in your section?

- A. Yes
- B. No

21. Have you ever seen any keeping of official documents or draft documents that contain identifying particulars of individuals as templates or sample case documents for future use in your section?

- A. Yes
- B. No

22. Have you ever seen any document containing Smart Identity Card Data not disposed of as classified wastes in your section?

- A. Yes
- B. No

23. Do you personally know of any case of missing documents/devices containing Smart Identity Card Data not being reporting to the supervisors in your section?

- A. Yes
- B. No

24. What will you do if you notice an unauthorized transfer/use of Smart Identity Card Data? (You may write your answer in Chinese or English.)

25. In your opinion, what can be done by ImmD to enhance the security of SMARTICS? (You may write your answer in Chinese or English.)

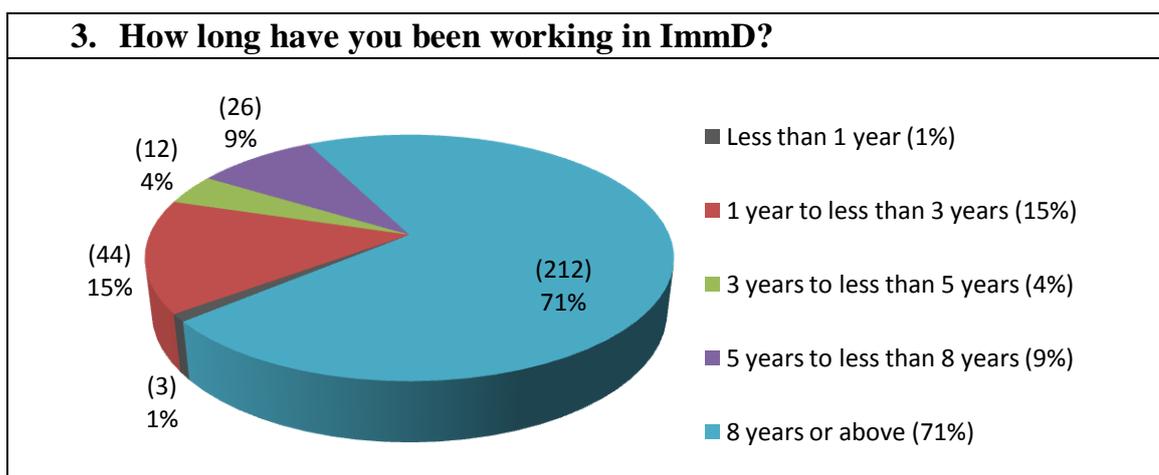
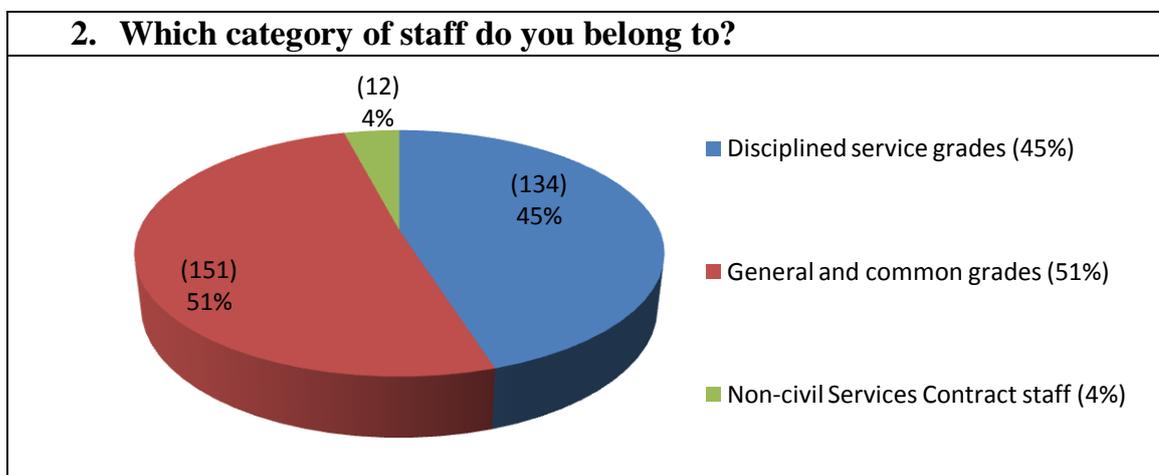
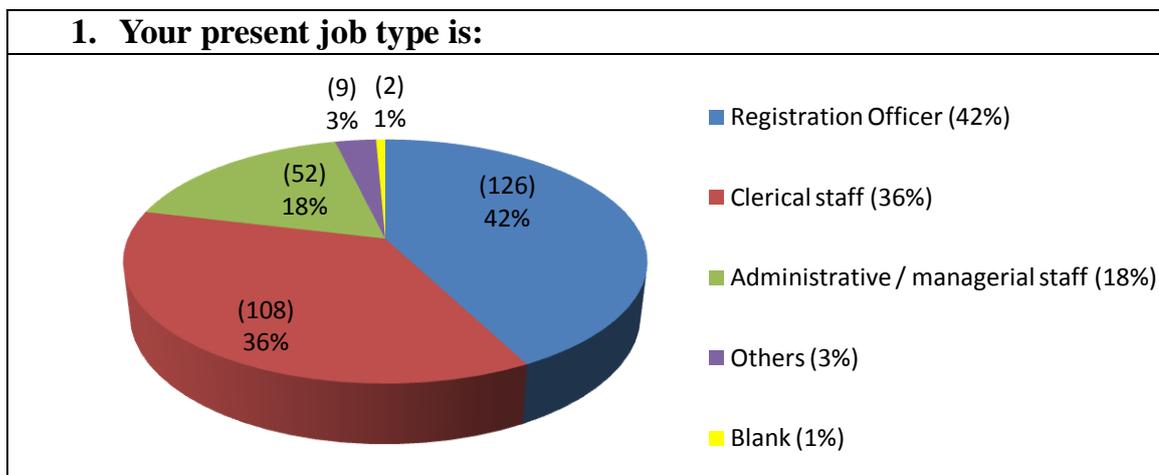
--- END ---

19. 你有沒有見過你部門中有人共同使用智能身份證系統的登入密碼？
A. 有
B. 沒有
20. 你有沒有見過你部門中有人使用智能身份證系統後沒有登出？
A. 有
B. 沒有
21. 你有沒有見過你部門中有人保留載有個人辨識資料的官方文件或文件草稿，作為日後使用的模版或樣本文件？
A. 有
B. 沒有
22. 你有沒有見過你部門中有人不依從處理機密廢料的程序把載有智能身份證資料的文件棄置？
A. 有
B. 沒有
23. 你是否知道你部門中曾否發生遺失載有智能身份證資料的文件/電子裝置而沒有向上司報告的事件？
A. 知道
B. 不知道
24. 當你知道有人未經准許移轉/使用智能身份證資料時，你會怎樣做？(你可用中文或英文作答。)

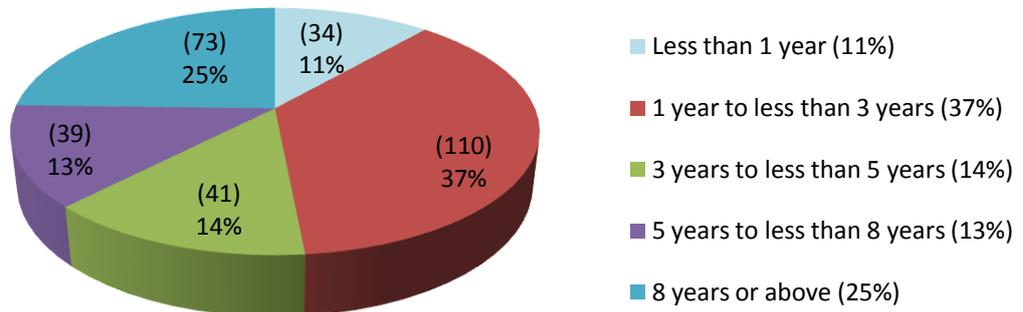
25. 你認為入境處可以如何提高智能身份證系統的保安？(你可用中文或英文作答。)

--- 完 ---

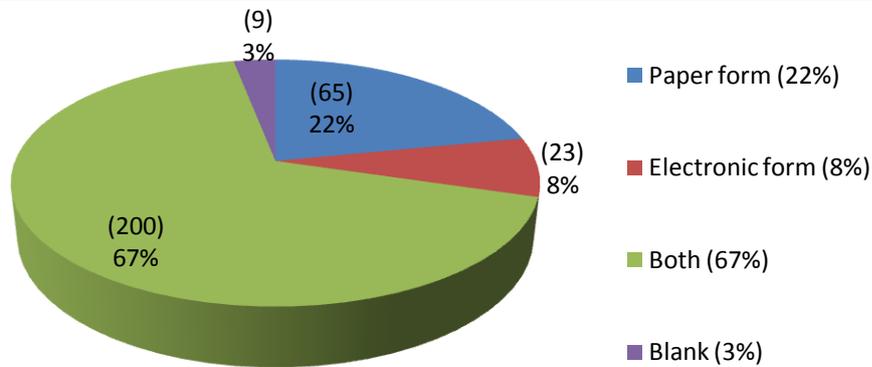
(B) Results analysis



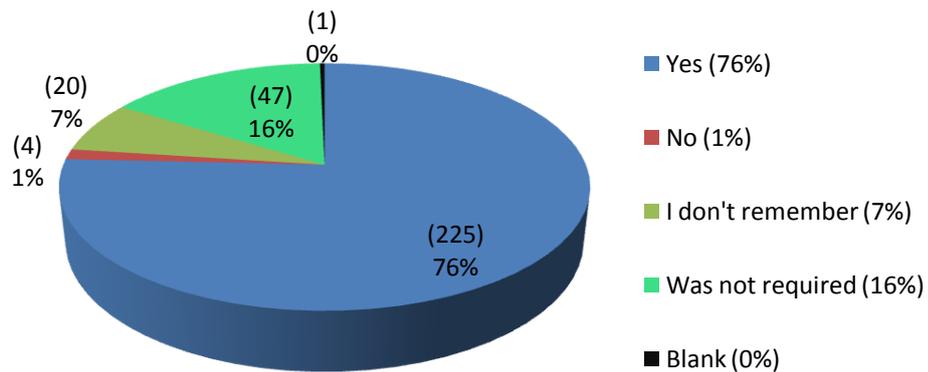
4. How long have you been working in your current section?



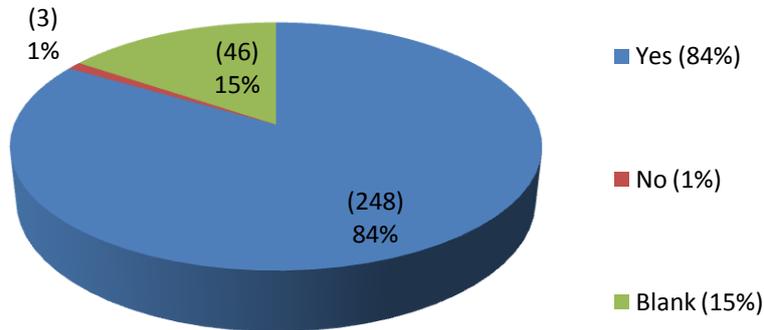
5. In the discharge of your job duties, what form of Smart Identity Card Data will you handle?



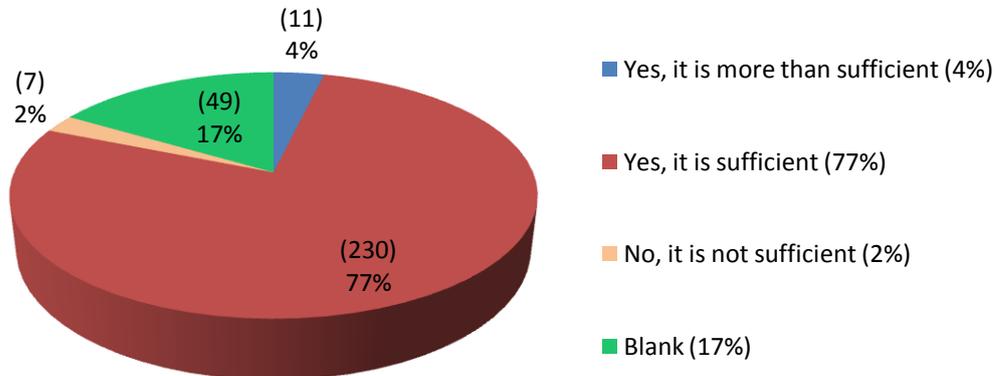
6. Were you required to sign an undertaking that you would comply with the SMARTICS security requirements when you received the user ID and password?



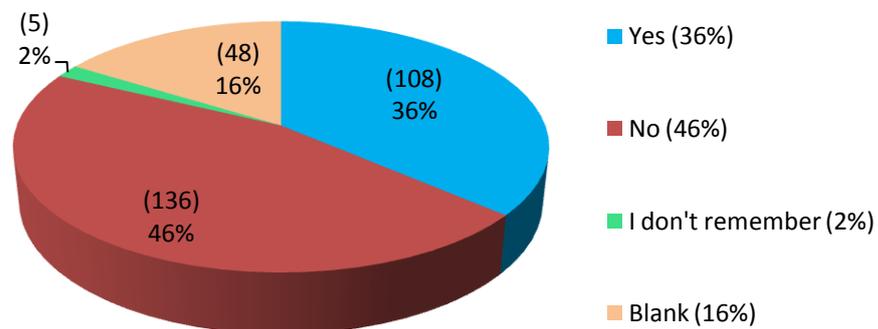
7. Are your access rights to SMARTICS commensurate with your job responsibilities?



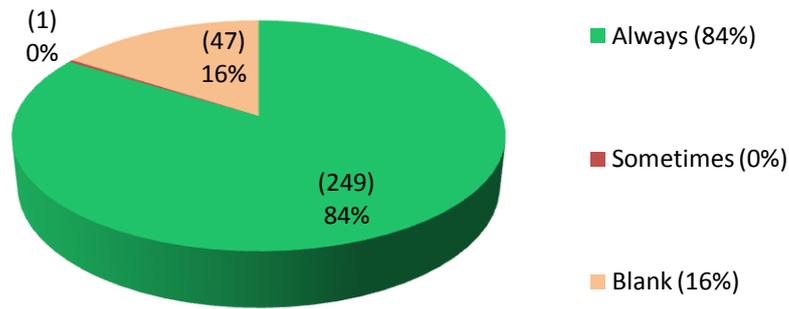
If yes, do you find your access rights to SMARTICS sufficient for performing your duties?



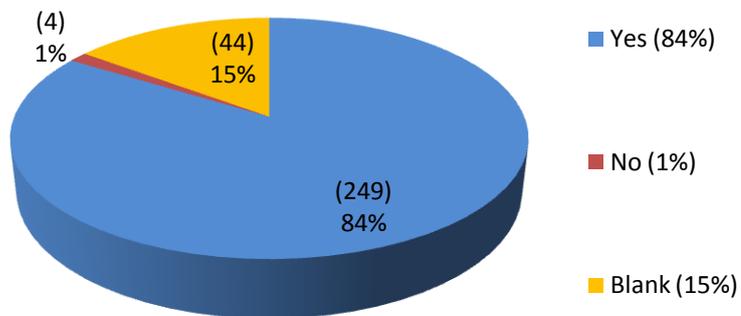
8. Have you ever changed your password for SMARTICS before the system prompts you to do so?



9. Do you log out SMARTICS whenever you leave your terminal?



10. Do you know that all of your transactions performed in SMARTICS are logged by the system?

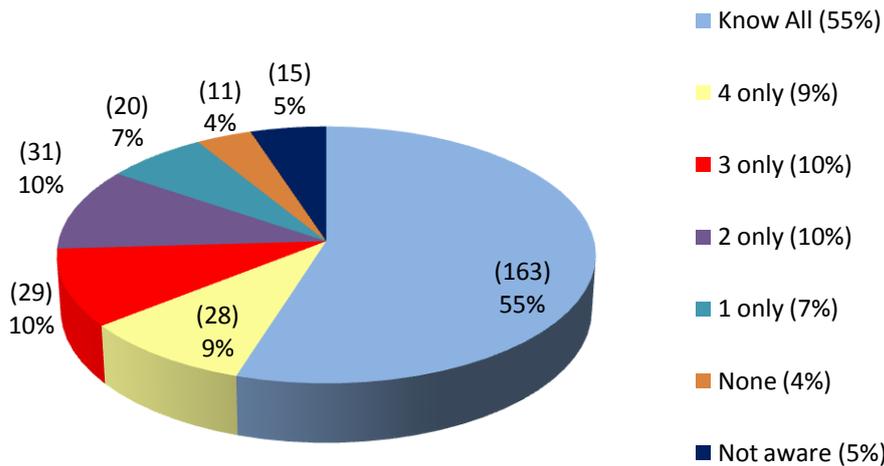


Remarks:

Only 81 respondents (36% of 225 SMARTICS users) know the 6-month retention period for audit trail report.

11. Have you ever read the following ordinance, policies, guidelines or practices of ImmD? (You may choose to tick more than one box)

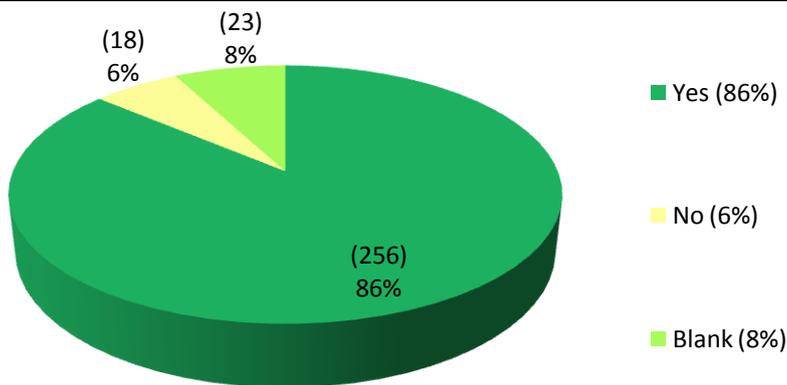
- Section 17 of the Official Secrets Ordinance
- Information Technology Security Policy for Immigration Department
- Information Technology Security Guidelines for Smart Identity Card System
- Immigration Department Circular No. 9/2008 – Compliance with Data Protection Principle 4 of Personal Data (Privacy) Ordinance
- Immigration Department Circular No. 2/2009 – Security in the Handling of Classified Documents
- No, I am not aware of any of the above



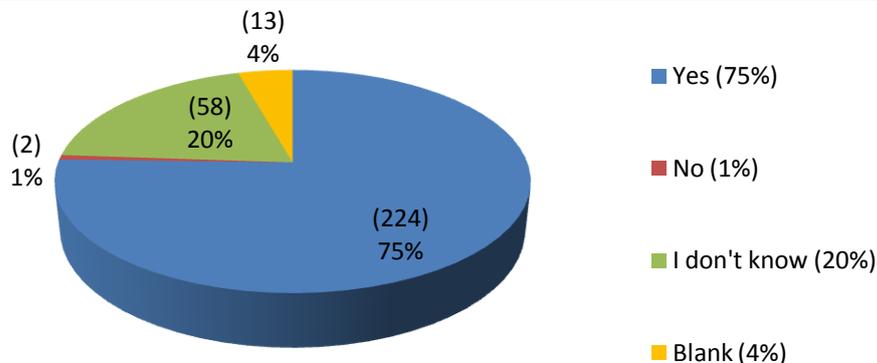
Remarks:

The most popular way to know the existence of the abovementioned documents was informed by their supervisors, either verbally or in writing whilst the least popular way was through intranet.

12. Does your supervisor follow the guidelines of ImmD to store away hard copies of Smart Identity Card Data when not in use?



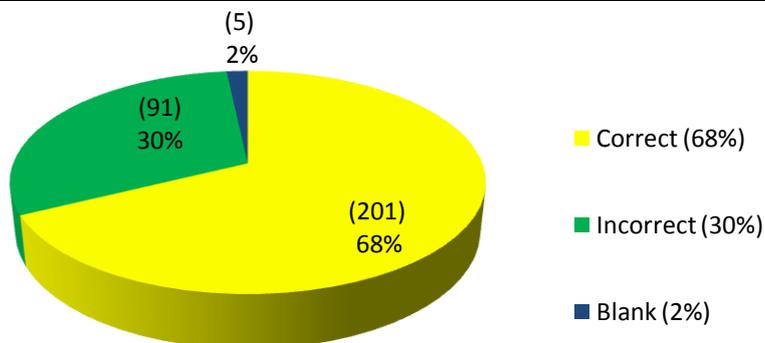
13. Does your supervisor regularly inspect if there is any hard copy of Smart Identity Card Data is retained longer than the period specified in the retention policy of ImmD?



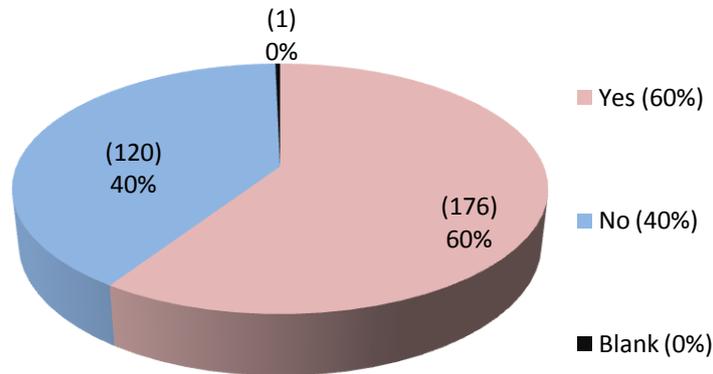
14. Which of the following is/are official classification(s) of Smart Identity Card Data? (You may choose to tick more than one box)

- Top Secret
- Secret
- Confidential
- Restricted
- General

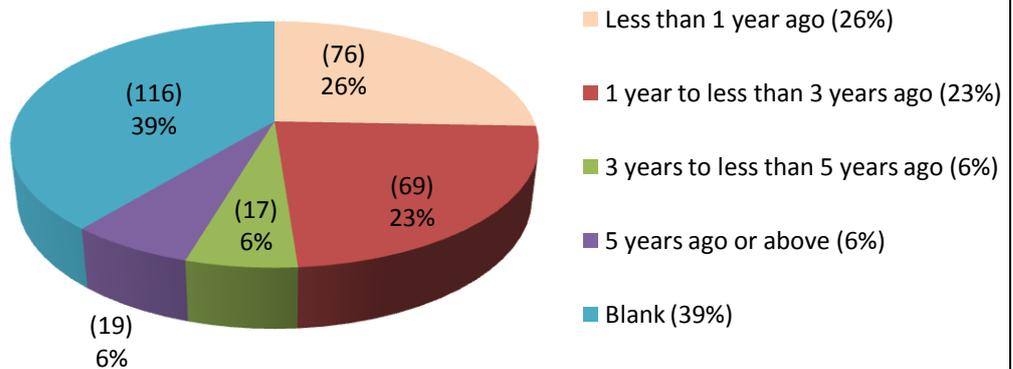
Note: The correct answer is “Confidential” and “Restricted”.



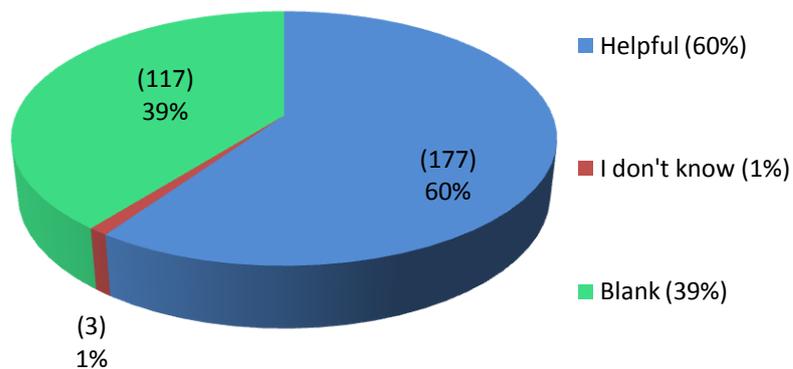
15. Have you attended a training session in personal data privacy protection?



If yes, when did you receive the last training?



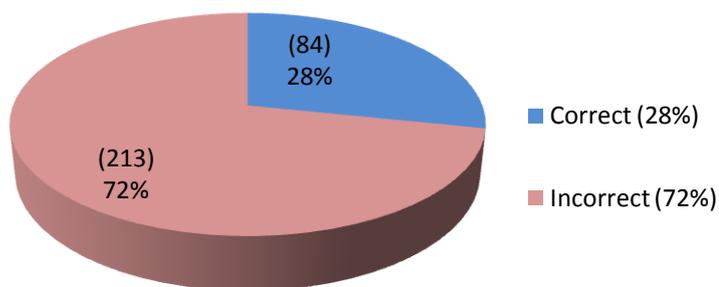
If yes, did you find the training helpful in addressing the security of Smart Identity Card Data?



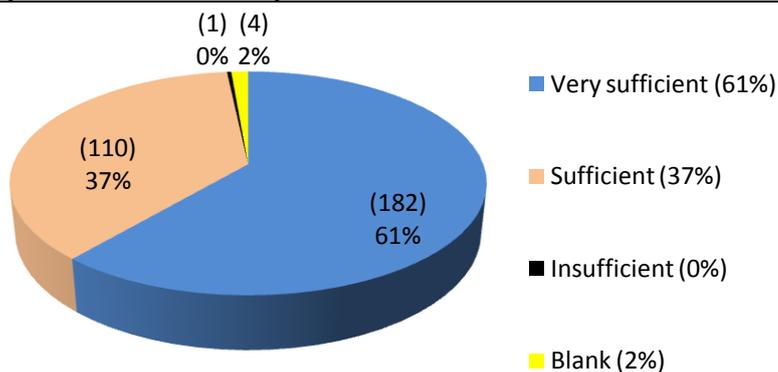
16. If a staff member reports to his supervisor that an application form ROP1 containing Smart Identity Card Data that was registered on 1 September 2008 and had not been disposed is missing, which of the following Data Protection Principle(s) of the Personal Data (Privacy) Ordinance might be involved? (You may choose to tick more than one box)

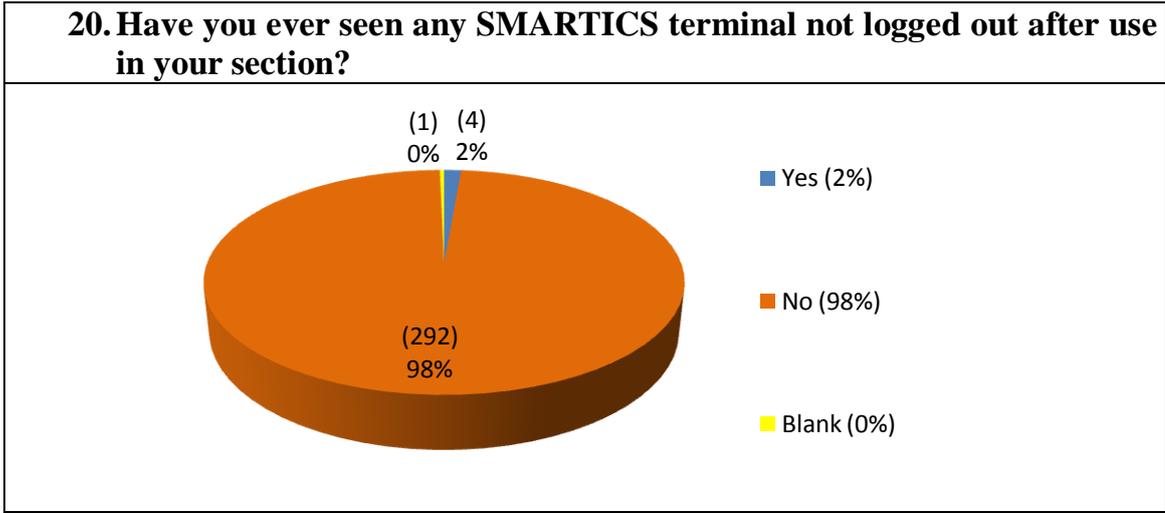
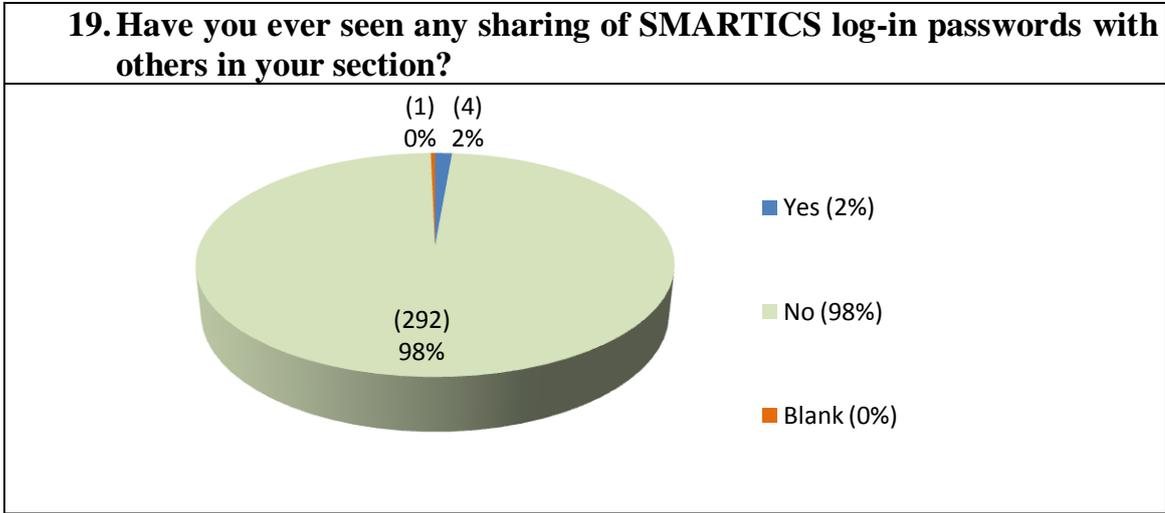
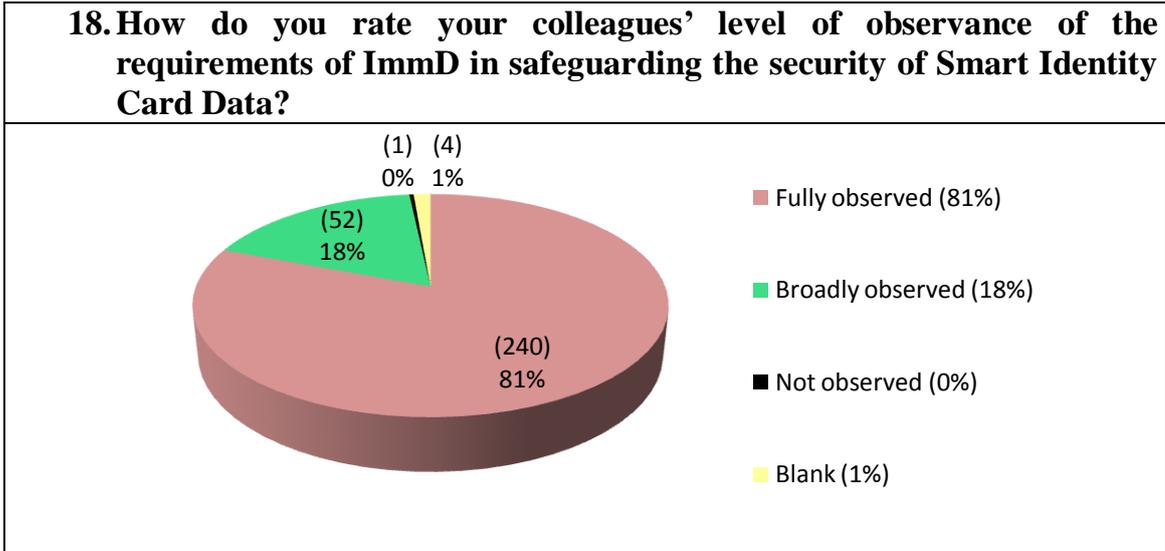
- Principle 1 – purpose and manner of collection of personal data
- Principle 2 – accuracy and duration of retention of personal data
- Principle 3 – use of personal data
- Principle 4 – security of personal data
- Principle 5 – information to be generally available
- Principle 6 – access to personal data
- None of the above
- I do not know

Note: The correct answer is “Principle 2” and “Principle 4”.

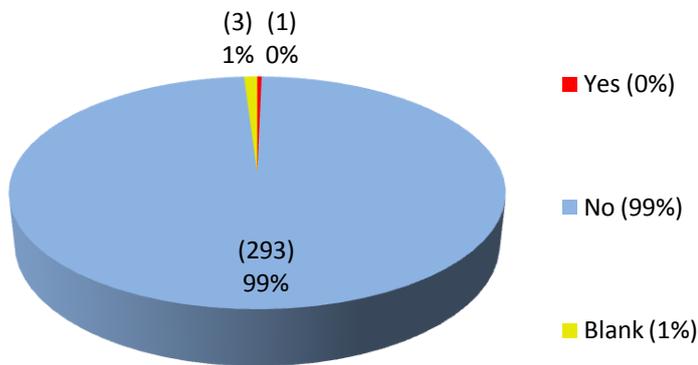


17. How do you rate the overall measures adopted by ImmD to protect the security of Smart Identity Card Data?

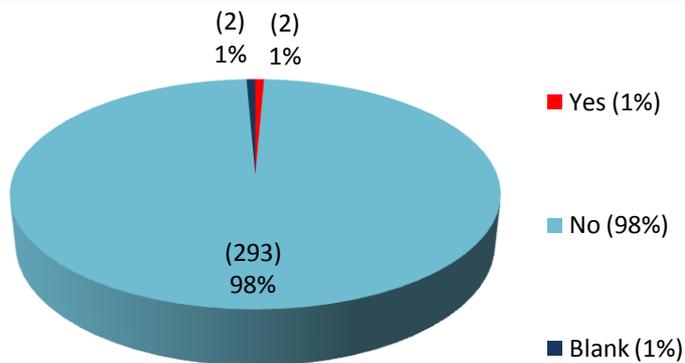




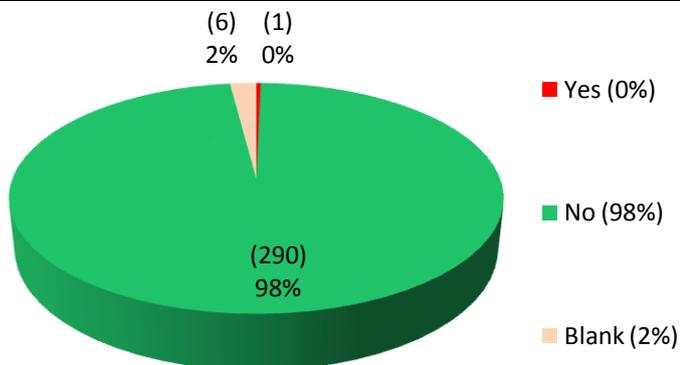
21. Have you ever seen any keeping of official documents or draft documents that contain identifying particulars of individuals as templates or sample case documents for future use in your section?



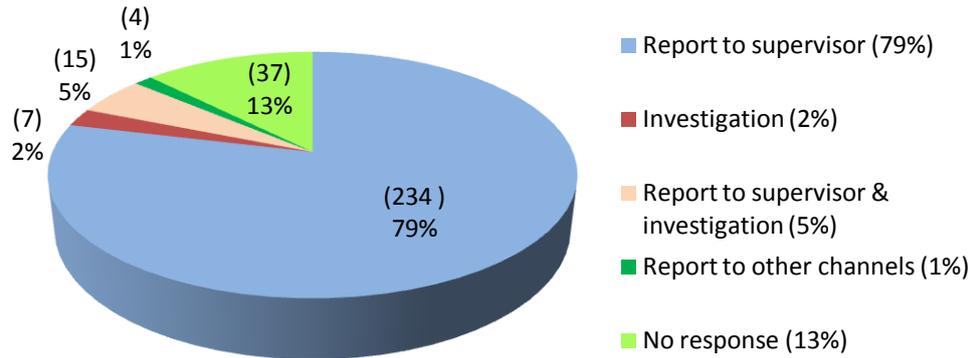
22. Have you ever seen any document containing Smart Identity Card Data not disposed of as classified wastes in your section?



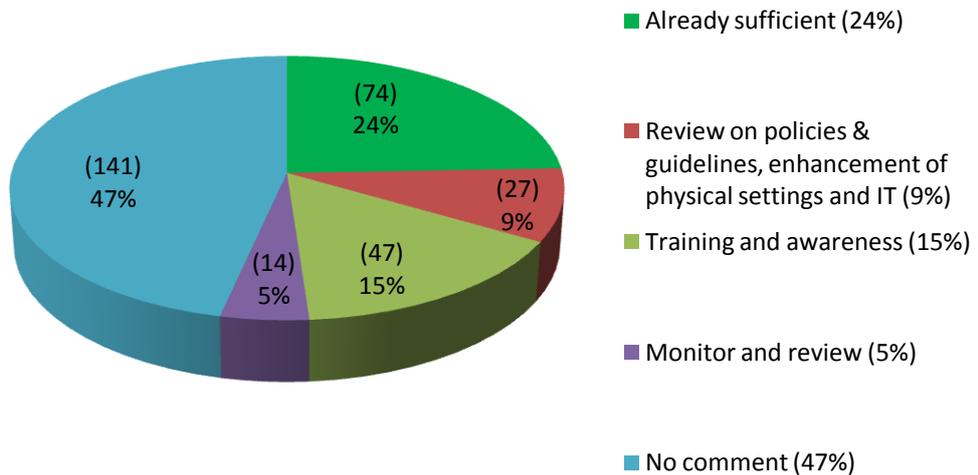
23. Do you personally know of any case of missing documents/devices containing Smart Identity Card Data not being reporting to the supervisors in your section?



24. What will you do if you notice an unauthorized transfer/use of Smart Identity Card Data?



25. In your opinion, what can be done by ImmD to enhance the security of SMARTICS?



Remarks:

Some respondents provide more than one answer to this question.

Remarks:

(1) There are altogether 300 submissions and only 297 are valid

(2) All figures are rounded off

Appendix VI – Photographs taken at Immigration Department



Picture 1 - Fingerprint reader at ROP Offices



Picture 2 - Shredding machine at ROP Offices



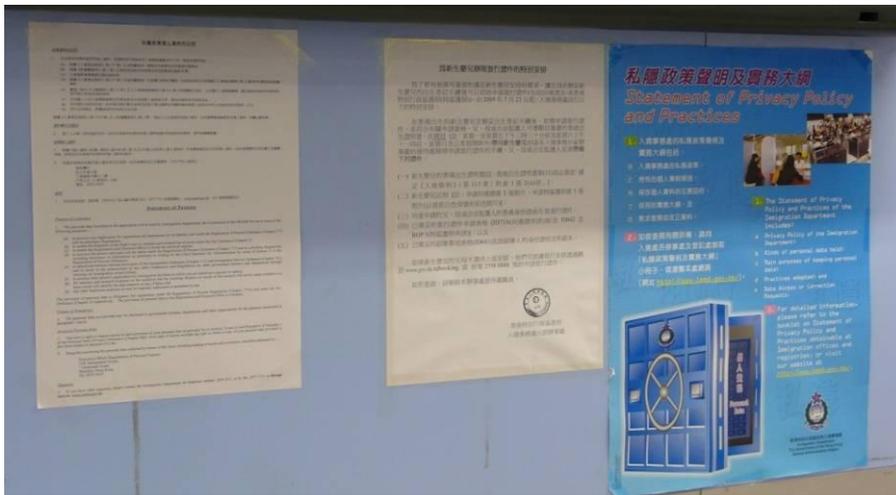
Picture 3- Metal Briefcase containing backup tapes of Smart ID Card Data



Picture 4 - Immigration Self-service kiosks at ROP Yuen Long Office



Picture 5 – Immigration Self-service kiosk at ROP Kwun Tong Office



Picture 6 – Privacy Policy and Statement of Purpose at ROP Yuen Long Office