Tutorial 6

InfoSec Policies and Governance

T1_G3

Done by: Chan Wei Ling, Kwek Chu Han, Tay Chin Heng, Wong Zhen Wei

Part I: Warm-up Questions

1. According to NUS IT Security Policy, users should familiarize themselves with NUS IT Security Policy and all other relevant security standards and procedures. Though in case by case situations, ignorance will be accepted as a valid reason for noncompliance

False

4.2.2 Users should familiarise themselves with NUS IT Security Policy and all other relevant security standards and procedures. Ignorance will not be accepted as a valid reason for non-compliance.

Part I: Warm-up Questions

2. According to NUS IT Security Policy, it adopts need-to-know and least privilege access control principles. Therefore, by default, School Dean should have access to each faculty member's account on LumiNUS and evaluate whether the grading is appropriately done, as the rank of School Dean is higher than faculty members' rankin the organization.

   False

   Since the School Dean only needs to know whether the grading is appropriately done, he/she only needs access to the member's grades and not the whole account. Therefore, this statement violates the least privilege access control principle.

Part I: Warm-up Questions

3. According to NUS IT Security Policy, dual control over the issue of access cards/keys to “secured areas” shall be in place

True

> 3.5.3 Dual control over the inventory and issue of access cards/keys to ‘secure areas’ shall be in place.

Part I: Warm-up Questions

4. According to NUS IT Security Policy, non-critical data should be backed up daily and stored in a secured off-site location.

False

6.2.5 Information systems data or functions are considered non-critical data if the unavailability of that information poses no disruption or minimal disruption of service to customers and vendors. Such information will be backed-up periodically and periodically moved to a secure off-site location.

Part I: Warm-up Questions

5. The agreement between NUS and suppliers may include which of the following requirements? (please select all the options that apply)

3.6.4 Agreement with Supplier may include the following requirements:

(a) Compliance obligations

(i) Regulatory

(ii) Contractual

(b) Service level agreement (e.g. Availability, Response time)

(c) Logical/physical access management

(d) Right to monitor and review (e.g. privilege accounts, accesses, system performance, logs, configurations, transactions)

(e) Right to audit (including sub-contractor)

All of the above

Part II: Discussion Question

1. **Introduce the following roles and corresponding responsibilities.**
    a. Data Owner
    b. Data Stewards
    c. Data Managers
    d. Data Custodian
    e. Data Users
    f. Data Governance Team

Part II Q1: Data Owner

National University of Singapore

- Ultimate responsibility for the stewardship of University Data
- Legal entity accountable for ensuring that the maintenance of and access to University Data are in accordance with ethical, legal, institutional and professional rules, regulations, and obligations.

DMP 3.0: 3.3 Shared Responsibility

Part II Q1: Data Stewards

Heads of Department

- Accountable for University Data within their functional area

  <u>Within functional area:</u>

- Responsible for the collection, use, maintenance, disposal and protection of University Data
- Ensure that the necessary data procedures and guidelines are put in place and are aligned with the Data Management Policy
- Appoint Data Managers and System Owners to assist in the day-to-day operational matters

DMP 3.0: Appendix B: 1. Data Stewards

Part II Q1: Data Managers

An NUS staff member (typically at the level of Manager and above or equivalent), appointed by the Data Steward

- Responsible for operational-level data management activities:
  - Creating, updating, archiving, disposing and securing the data
  - Understanding and maintaining the definition, purpose, use and classification of the data
  - Ensuring the quality and accuracy of the data
  - Authorising access to the data according to the Policy approval process
  - Handling of data sharing with Data Users or data disclosure to External Parties
  - Providing data requirements to System Owners
- Carry out above responsibilities and develop data procedures and guidelines for their function and department in consultation with the Data Steward

DMP 3.0: Appendix B: 2. Data Managers

Part II Q1: Data Custodian

An NUS Staff member (typically playing the role of an IT function) who owns the technical accountability for University Data

- Responsible for the technical management of the data.
- Responsible for the technical platform hosting University Data including its technology, design, modelling, technical maintenance and support.

DMP 3.0: Appendix B: 4. Data Custodian

Part II Q1: Data Users

Any person who has access to University Data to do work for NUS

- Include NUS Staff and Non-NUS Staff
- NUS Staff responsible for the hiring or engagement of Non-NUS Staff must ensure that the Non-NUS Staff are bound by a Non-Disclosure Agreement (NDA) or equivalent terms and conditions.
- NUS Staff must ensure the Non-NUS Staff uphold the principles of Data Management Policy and the instructions specified on use of University Data.

DMP 3.0: Appendix B: 5. Data Users

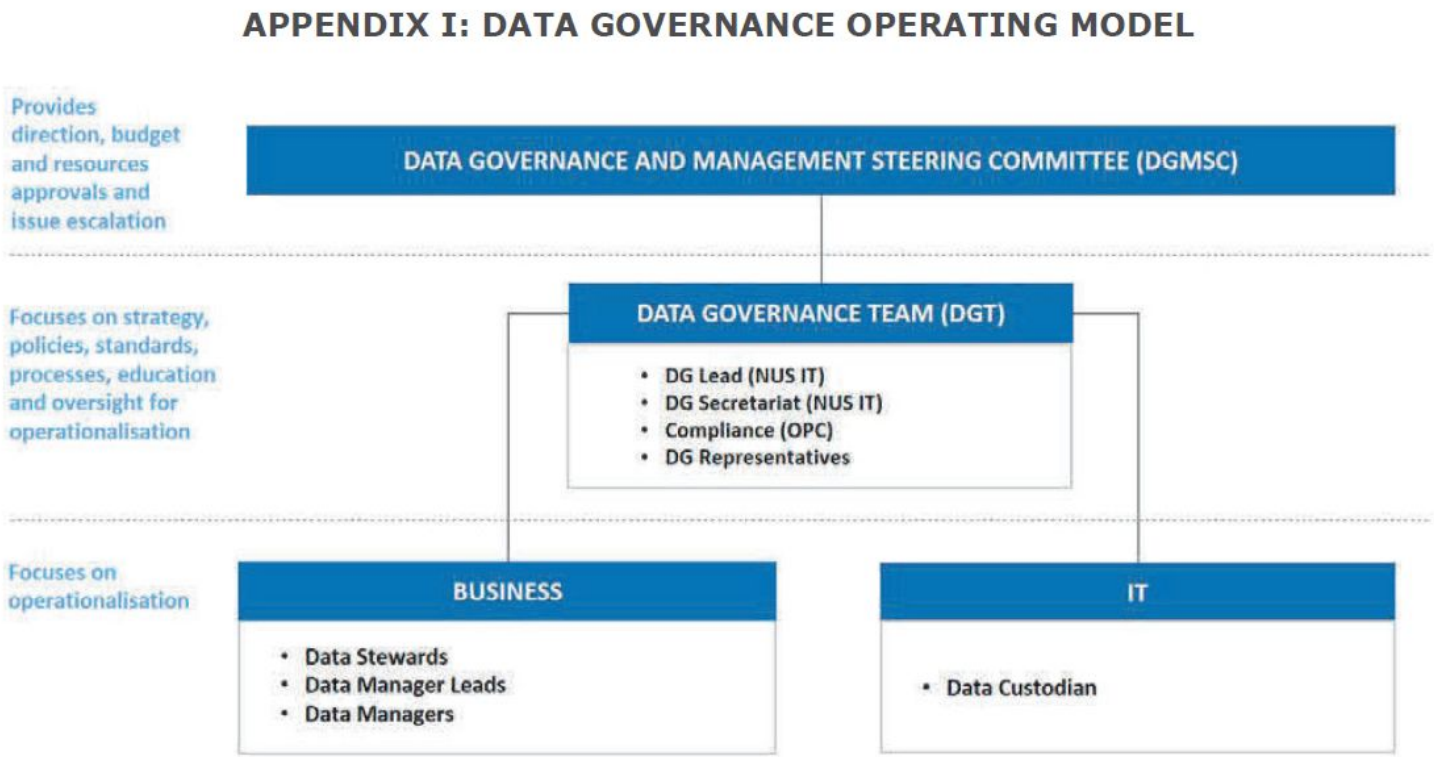
Part II Q1: Data Governance Team

Management working committee

- Develops the enterprise data strategy including policies, standards and processes for the appropriate management of University Data
- Determine key data sets (Master Source data) to facilitate a single source of truth for Data Sharing

DMP 3.0: Appendix I: 1. Data Governance Operating Model

Part II Q1: Data Governance Team



Part II Q1: Data Governance Team

DG Lead

- Define enterprise data management strategy
- Champion data management initiatives across the enterprise
- Accountable for data governance budget
- Resolve data related issues/risks (Decide solution)
- Engage DGMSC for awareness campaigns

DMP 3.0: Appendix I: 1. Data Governance Operating Model

Part II Q1: Data Governance Team

DG Secretariat

- Facilitate and support NUS' data governance administrative matters.
  - Manage communication between DGMSC and stakeholders
  - Ensure proper logistics for Data Governance initiatives and activities
  - Prepare qualitative agendas and minutes for the DGMSC
  - Maintain relevant records of DGMSC decisions

DMP 3.0: Appendix I: 1. Data Governance Operating Model

Part II Q1: Data Governance Team

DG Representatives

- Work closely with the DG Lead to drive data management initiatives across the enterprise
- Manage communication for processes and policies within their respective cluster and departments
- Resolve data related issues/risks (Provide solutions)

DMP 3.0: Appendix I: 1. Data Governance Operating Model

Part II: Discussion Question

2. Using the seven successful policy characteristics to evaluate NUS IT Security Policy, which characteristic causes the **most doubt/challenge** for this policy's success?
    a. Endorsed
    b. Relevant
    c. Realistic
    d. Attainable
    e. Adaptable
    f. Enforceable
    g. Inclusive

Part II: Discussion Question

2. Using the seven successful policy characteristics to evaluate NUS IT Security Policy, which characteristic causes the **most doubt/challenge** for this policy's success?
    a. Endorsed
    b. Relevant
    c. Realistic
    d. Attainable
    e. Adaptable
    f. Enforceable
    g. Inclusive

Part II Q2: Endorsed

- NUS has a dedicated committee that aims to provide high level support and commitment for NUS information security initiatives.
- Management of NUS IT sets strategic direction and provides support for information security initiatives.

Information Security Organisation

3.1 NUS IT Steering Committee

3.1.1 NUS IT Steering Committee is chaired by Provost and Deputy President and comprises of members from key departments. This committee provides high level support and commitment for NUS information security initiatives.

3.2 Information security responsibilities

3.2.1 Management of NUS IT sets strategic direction for NUS information security initiatives and provides support, commitment and resources for NUS information security initiatives.

Part II Q2: Relevant

- Each policy has a well-defined scope that states the purpose of its implementation as well as the goal it intends to achieve.

Chapter 4 NUS IT Security Policy: Access Control Security

1 **Purpose and scope**
This chapter defines the control requirements for access to NUS information system resources.

Chapter 8 NUS IT Security Policy: Operations Management

1 **Purpose and scope**
The purpose of this chapter is to establish standards that aim to reduce the risk of errors and security compromises occurring during systems processing by careful control of system operations.

Part II Q2: Realistic

- The Introduction to IT Security Policy states that threats from various sources have become more common and increasingly sophisticated.
  - This builds on the realistic goal of protecting the organisation from emerging threats by implementing a set of security measures.
- Some examples of security measures implemented are:
  - Risk Analysis, Incident Management, Access Control Security, Physical Security etc
- The security policy also considers the technical feasibility of a system. E.g:
  - "**Where technically feasible**, systems and applications must use password history techniques to maintain a history of used passwords." (C4 Section 4.1.6)

Part II Q2: Attainable

- All security measures stated in the policy have well-defined standards, guidelines, practices and procedures to comply with the given policy.
- Standards
  - “Where technically feasible, systems and applications should be configured to only accept passwords that are of a minimum of eight (8) characters in length and be comprised of letters, numbers, and/or special characters” (C4 Section 4.1.4)
- Guidelines
  - “Users should adhere to good practices in the selection and use of passwords. Dictionary words and passwords that can be easily associated with himself or herself should be avoided.” (C4 Section 5.5.1)
- Practices
  - “The review of user access rights should be conducted every twelve (12) months to revoke rights that are no longer required by users.” (C4 Section 4.4.2)
- Procedures
  - “Procedures for job execution should be documented” (C8 Section 3.1 Documented Operating Procedures)

Part II Q2: Adaptable

- The security policies defined are generally adaptable to new technological changes. Some examples include:
  - "NUS IT Security Policy must be reviewed every twelve (12) months and whenever there are changes in the security strategies in NUS." (C3 Section 3.3.1)
  - "All Standard Operating Procedures (SOPs), procedures, guidelines and documentations, etc shall be reviewed every twelve (12) months and whenever there are major changes in the scope of work." (C3 Section 3.4.1)
  - "All special or privileged access to systems (such as administrative or supervisor accounts at the application or system level) must be reviewed every twelve (12) months or when major changes are made to the IT systems." (C4 Section 4.4.1)
- Consistent review of policies will allow NUS to adapt to emerging threats.

Part II Q2: Inclusive

- The security policy generally applies to all individuals who are part of / working with NUS. These include:
  - NUS Students
  - NUS Staff
    - Professors, System Administrators etc
  - External Parties
    - IT Vendors, Contractors, Auditors

Intended audience

3.2.1 This IT Security Policy is intended to be read by all staff and students of NUS and all other external parties that have dealings with NUS information system resources, including the use, design, audit, implementation and maintenance of these resources.

Part II Q2: Enforceable

- Probably the most challenging characteristic to succeed
- There exists a Compliance policy to ensure enforcement of rules
- However, there are some standards that may be difficult to enforce:
  - "Users should not reveal their passwords or share the use of their accounts with anyone."
  - "Users should adhere to good practices in the selection and use of passwords. Dictionary words and passwords that can be easily associated with himself or herself should be avoided."
- Certain policies may not be well-enforced due to human error
  - "In situations where user with access to sensitive information is terminated, the employee's immediate supervisor must ensure timely removal of the user's access rights."

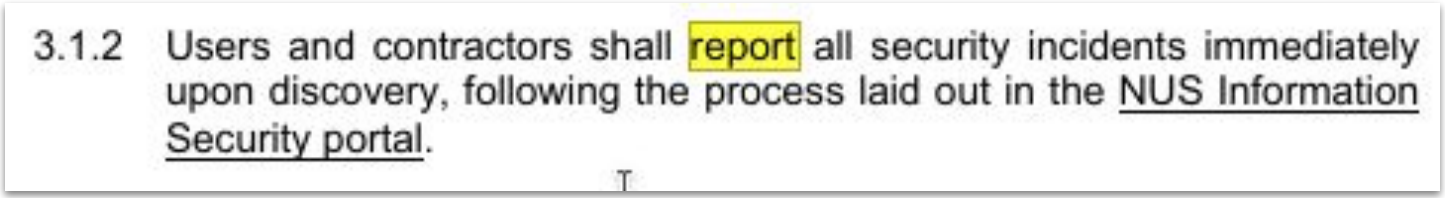
Part II: Discussion Question

3. Read the section of Information Security Governance Maturity Model in “Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition” from ISACA (i.e., Information Systems Audit and Control Association) (p.36-p.39) and answer the following questions:
   a. Briefly introduce the model
      This is a model for boards of directors and executive management to establish rankings for their organisation’s maturity in IT.
   b. Based on your reading of NUS information security related policies and your daily observation on InfoSec management on campus, assess NUS information security governance management, which maturity level does NUS meet?

      Between 3 and 4

Part II: 3B

- Risk management is developed and clearly defined under the **NUS IT Security Policy, Chapter 2**
- Formal security reporting procedure is formed.
  Incident management (Chapter 9):



- NUS have periodic security assessments to evaluate the effectiveness of implementation of the security plan
  - As mentioned in their background, they “ran regular checks on its systems... detected unauthorized intrusion into its IT systems on 11th April, during cybersecurity assessments by external consultants...:”

Part II: 3B

- Authorisations are in-place based on least-privilege principle

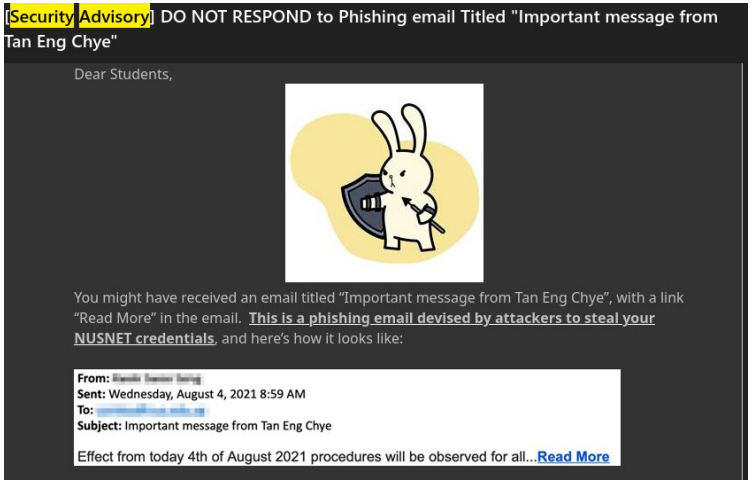
Access Control Security (Chapter 4):

4.3 Privileges and rights management

4.3.1 Authorisation for privileged application or system level (e.g. administration accounts for operating systems, databases or applications or accounts that can override system or application controls) access must be obtained from relevant management staff responsible for the IT platform of system, prior to access being given. These privileges must be based on functional or job necessity and must only be allocated on a need-to-have basis. If it is mutually agreed that the Data Manager approval is to be obtained in place of that of the management staff responsible for the IT platform or system, it should be documented accordingly.

Part II: 3B

- Access to NUS systems generally requires identification and authentication through a Single-Sign-On (SSO) portal
  - https://vafs.nus.edu.sg
- Security Advisory are given in the face of new threats

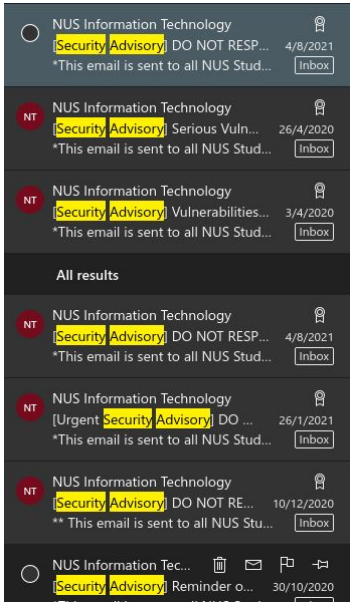

[Security Advisory] DO NOT RESPOND to Phishing email Titled "Important message from Tan Eng Chye"

Dear Students,

You might have received an email titled "Important message from Tan Eng Chye", with a link "Read More" in the email. **This is a phishing email devised by attackers to steal your NUSNET credentials**, and here's how it looks like:

From: [redacted]
Sent: Wednesday, August 4, 2021 8:59 AM
To: [redacted]
Subject: Important message from Tan Eng Chye

Effect from today 4th of August 2021 procedures will be observed for all...Read More



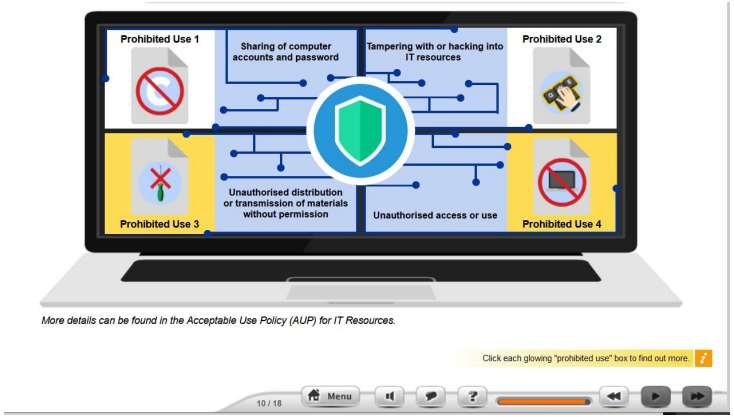
Part II: 3B

- Responsibilities for IT are clearly assigned, managed and enforced
  - Overview: **NUS IT Security Policy Chapter 3 Section 3 Information Security Organisation**
  - Detailed information: **NUS Data Management Policy**
- Prompt and appropriate response in face of intrusions
  - As noted in the background section of the tutorial

Part II: 3B

- Security awareness briefings are mandatory
  - Students: SE1000 Students Essential
  - Staff and others: Believed to have since they have access to more sensitive information

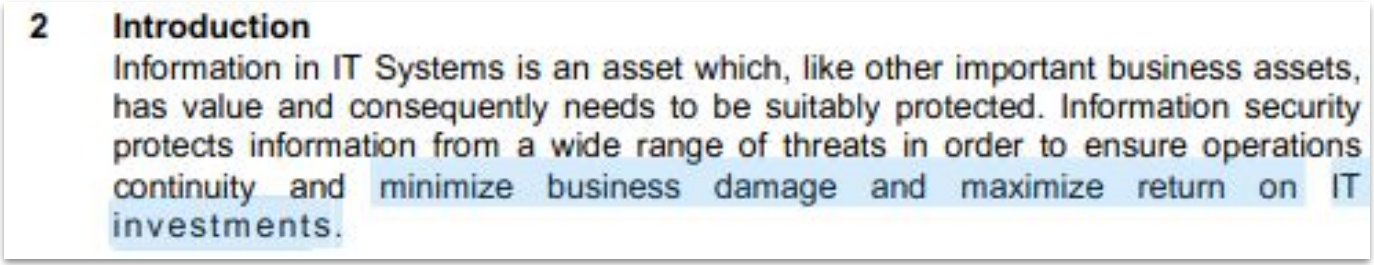
  (Prof add that this is lacking)



Part II: 3B - Why not 4?

- Lack of cost-benefit analysis

  Introduction to Information Technology (IT) Security Policy (Chapter 1):



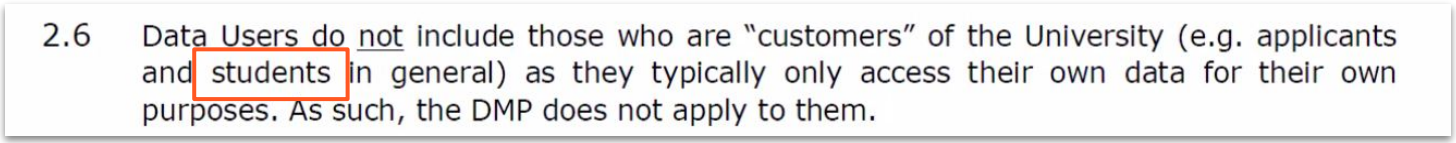
2 Introduction

Information in IT Systems is an asset which, like other important business assets, has value and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure operations continuity and minimize business damage and maximize return on IT investments.

Part II: 3B - Why not 5?

- Lack of continuous service plans and business continuity plans
- Risk management may not be organisation-wide and may not always be followed regularly or managed well
    - Applicants or students are excluded

      NUS Data Management Policy 3.0:



2.6 Data Users do not include those who are "customers" of the University (e.g. applicants and students in general) as they typically only access their own data for their own purposes. As such, the DMP does not apply to them.

Questions ?