IS4231
Information Security Management

Lecture 4

InfoSec Policies

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 4

Learning Objectives

- Describe the three major types of information security policy and discuss the major components of each
  - Enterprise information security program policy
  - Issue-specific security policy
  - System-specific security policy

What are Information Security Policies?

- Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets

  Audience are for the other employees in the company

  - Stipulate what is proper behavior when using information and information assets
  - Provide structure in the workplace
  - Create a productive & effective work environment, free from unnecessary distractions and inappropriate actions
  - Essential foundation of an effective InfoSec program

- Policies are the least expensive means of control and often the most difficult to implement

What are Information Security Policies? (cont.)

"*Policies are important reference documents for internal audits and for the resolution of legal disputes about management's due diligence, and policy documents can act as a clear statement of management's intent*"

-Information Security Policies Made Easy

For the SingHealth data breach - there are already flaws at a policy level

Spheres of Security

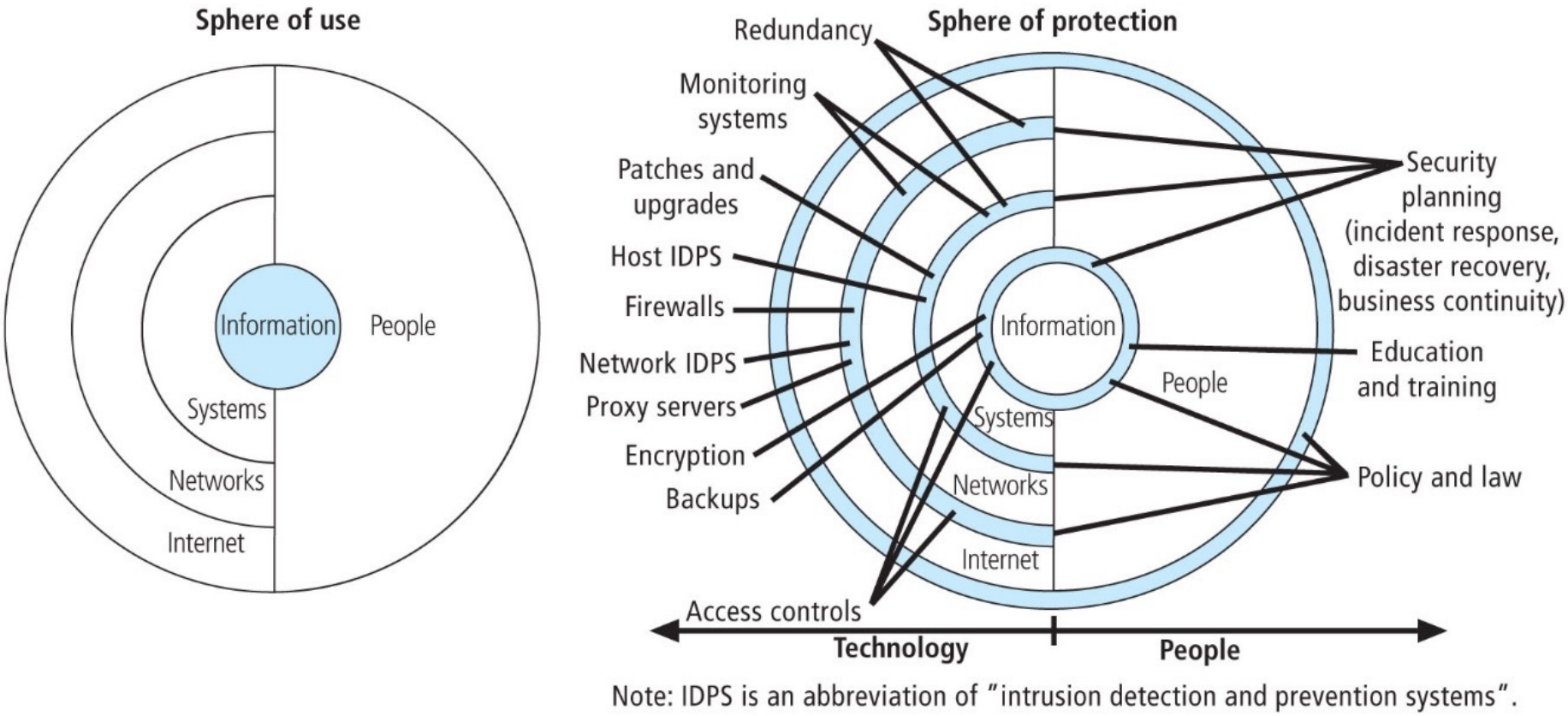


Figure 4-1 Spheres of security

Basic Rules and Guidelines

- Some basic rules when shaping a policy:
  - Policy should never conflict with law
  - Policy must be able to stand up in court if challenged
  - Policy must be properly supported and administered

- Guidelines help the formulation of IT and InfoSec policy:
  - All policies must contribute to the success of the organization
  - Management must ensure the adequate sharing of responsibility for proper use of information systems
  - nd users of information systems should be involved in the steps of policy formulation

Policy, Standards, and Practices (cont.)

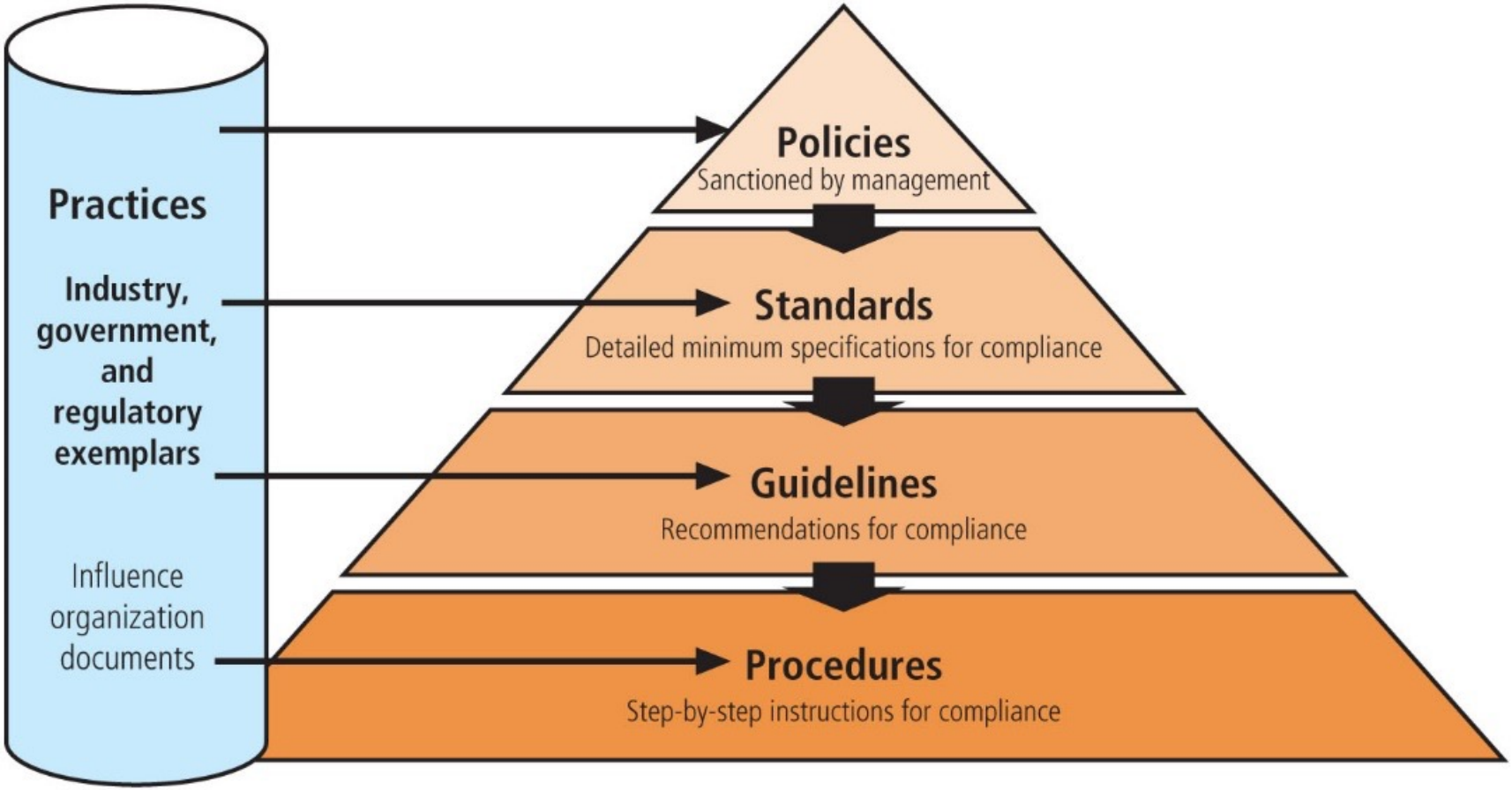


Figure 4-3 Policies, standards, practices, procedures, and guidelines

Policy, Standards, and Practices

- **Policies**: define what you can do and can not do, whereas the other documents focus on the how
- **Standards**: A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance.
- **Practices, procedures, and guidelines:** explain how employees are to comply with policy.

Example

Need all to have a complete set - to ensure that everyone, including those who are not as competent using tech are able to understand and follow

- Policy:
  - Use strong passwords, frequently changed
- tandard:
  - Must be at least 8 characters, with at least one number, one letter, and one special character
- Guideline:
  - "We recommend you don't use family or pet name, or parts of your birthday information, phone number in your password"
- Practices
  - Change semi-annually
- Procedures
  - Step-by-step instructions "first click Windows Start button, then…"

Current cloud policies

if there is a need to trust the end users to be honest, then it might not be too successful

Successful Policy Characteristics

- Endorsed
  - Management supports the policy
- Relevant
  - The policy is applicable and supports the goals of the organization
- Realistic
  - The policy makes sense
- Attainable
  - The policy can be successfully implemented
- Adaptable
  - The policy can be changed
- Enforceable
  - Controls that can be used to support and enforce the policy exist
- Inclusive
  - The policy scope includes all relevant parties

Three types of InfoSec Policies

- A complete Infosec policy must define three types of information security policy:
  - Enterprise information security program policy
  - Issue-specific information security policies
  - Systems-specific policies

- Based on NIST's "Special Publication 800-14"
  - NIST: National Institute of Standards and Technology
  - Outlined what is required of senior managers when writing InfoSec policy

Enterprise information security program policy (EISP)

What is an EISP?

- EISP
  - The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts.
- Also knowns as
  - Security program policy
  - General security policy
  - IT security policy
  - High-level InfoSec policy
  - InfoSec policy
- Must directly support the organization's vision and mission statements.

EISP Elements

- EISP documents should include:
  - An overview of the corporate philosophy on security
  - Information on the structure of the InfoSec organization and individuals who fulfill the InfoSec roles
  - Fully articulated responsibilities for security that are shared by all members of the organization (employees, contractors, consultants, partners, and visitors)
  - Fully articulated responsibilities for security that are unique to each role within the organization

EISP Elements

Table 4-1 Components of the EISP

Component	Description
Purpose	Answers the question, "What is this policy for?" Provides a framework that helps the reader to understand the intent of the document. Can include text such as the following, which is taken from Washington University in St. Louis: *This document will:* • *Identify the elements of a good security policy* • *Explain the need for information security* • *Specify the various categories of information security* • *Identify the information security responsibilities and roles* • *Identify appropriate levels of security through standards and guidelines* *This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.*[5]
Elements	Defines the whole topic of information security within the organization as well as its critical components. For example, the policy may state: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology" and then identify where and how the elements are used. This section can also lay out security definitions or philosophies to clarify the policy.
Need	Justifies the need for the organization to have a program for information security. This is done by providing information on the importance of InfoSec in the organization and the obligation (legal and ethical) to protect critical information, whether regarding customers, employees, or markets.
Roles and responsibilities	Defines the staffing structure designed to support InfoSec within the organization. It will likely describe the placement of the governance elements for InfoSec as well as the categories of individuals with responsibility for InfoSec (IT department, management, users) and their InfoSec responsibilities, including maintenance of this document.
References	Lists other standards that influence and are influenced by this policy document, including relevant federal and state laws and other policies.

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

Purpose and Scope

1 Purpose and scope

The purpose of this Policy is to define the minimum security measures required for the protection of information systems as well as the information contained and processed by the systems. These controls are described throughout the remaining sections of the Policy.

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.

The National University of Singapore (NUS) information systems landscape comprises of a broad range of information systems from personal Internet/Intranet web servers to highly sensitive and critical corporate systems. The systems have different characteristics in the following key areas:

- Sensitivity of information
- Criticality to operations of the University, Departments and Faculties
- Risk exposure
- Potential impact to NUS in the event of a security breach

The implementation and management of the security of this diverse range of systems, with varying security requirements, throughout the entire system life cycle, will be addressed by the NUS IT Security Policy.

The Policy defines security measures so that NUS information assets are protected and consistency in the implementation and practice of security throughout NUS can be achieved.

3.2 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.

Definition of information security

3.3 Key security objectives

3.3.1 Information security is characterized here as the preservation of three key security objectives:

- Confidentiality: ensuring that information is accessible only to authorized users;
- Integrity: safeguarding the accuracy and completeness of information and information processing systems;
- Availability: ensuring that authorised users have access to information and associated assets when required.

Need for information security

Increasingly, organizations and their information systems and networks are faced with security threats that attempt to compromise one or more of the above security objectives. These threats, from a wide range of sources, include computer-assisted fraud, espionage, sabotage, vandalism, fire or flood, computer viruses, computer hacking and denial of service attacks. Incidents and attacks arising from such threats have become more common and attacks have become more ambitious and increasingly sophisticated.

Philosophies

Information security is a process, which is achieved by implementing a suitable set of security measures, covering physical, environmental, personnel, technical and organisation structures security standards and procedures. These controls, as defined in the NUS IT Security Policy together with more detailed security procedures and guidelines, need to be established to ensure that NUS information systems and assets are adequately protected from a wide range of security threats.

Compliance

3.4 Non-compliance

3.4.1 Every staff, student and external party that has dealings with NUS information system resources is responsible for protecting and preserving the information in accordance with NUS IT Security Policy

Non-compliance with NUS IT Security Policy is viewed seriously and will result in disciplinary action up to and including legal action and termination.

Chapter 3 NUS IT Security Policy: IT Security Management

1 Purpose and scope

This chapter defines the various roles within NUS that are assigned responsibilities pertaining to the protection of information resources.

2 Introduction

Everyone associated with NUS has a role in information security. Due care must be exercised in the protection of IT information resources by clearly defining roles and responsibilities of management and users relating to information security.

3 Information Security Organisation

Governance

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.

Responsibilities

3.2 Information security responsibilities

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

Unique roles

3.2.2 Please refer to the NUS Data Management Policy for the details of the roles and responsibilities of the following:

Data Owner
Data Stewards
Data Managers
System Owners
Data Users
Data Administrators
Database Administrators
Application Developers
Infocomm Security Group

3.2.3 All systems shall be owned by the respective business/operating units and not by the IT Department.

Even for data users, there must be policies in place to ensure data users are accountable for any misconduct

Students are not considered owners - even the students emails/work/research paper

Domains

Table of Contents

Issue-Specific Security Policy (ISSP)

What is an ISSP?

- ISSP
  - An organization policy that provides detailed, targeted guidance to instruct all members of the organization in the use of **a resource**, such as one of its process or technologies.
  - Referred to as *fair and responsible use* policies

- An effective ISSP SOP
  - It articulates the organization's expectations about how its technology-based system should be used
  - It documents how the technology-based system is controlled and identifies the processes and authorities that provide this control
  - It indemnifies the organization against liability for an employee's inappropriate or illegal use of the system

What is an ISSP? (cont.)

- Every organization's ISSP has three characteristics:
  - Address specific technology-based systems
  - Require frequent updates
  - Contain an issue statement on the organization's position on an issue

ISSP Topics

- Use of electronic mail, IM, and other communications apps
- Use of the Internet, the Web, and company networks by company equipment
- Malware protection requirements
- Use of nonorganizationally issued software or hardware on organization assets
- Use of organizational information on nonorganizationally owned computers
- Prohibitions against hacking or testing security controls or attempting to modify or escalate privileges
- Personal and/or home use of company equipment
- Removal of organizational equipment from organizational property
- Use of personal equipment on company networks (BYOD)
- Use of personal technology during work hours
- Use of photocopying and scanning equipment
- Requirements for storage and access to company information while outside company facilities
- Specifications for the methods, scheduling, conduct, and testing of data backups
- Requirements for the collection, use, and destruction of information assets
- Storage of access control credentials by users

ISSP Elements

- **Statement of Purpose**: outline the scope and applicability of the policy
  - Scope and Applicability
  - Definition of Technology Addressed
  - Responsibilities
- **Authorized Access and Usage of Equipment**: explain who *can* use the technology governed by the policy and by what purposes
  - User Access
  - Fair and Responsible Use
  - Protection of Privacy
- **Prohibited Usage of Equipment**: outlines what it *cannot* be used for
  - Disruptive Use or Misuse
  - Criminal Use
  - Offensive or Harassing Materials
  - Copyrighted, Licensed or other Intellectual Property
  - Other Restrictions
- **Systems Management**: specify users' and systems administrators' responsibilities
  - Management of Stored Materials
  - Employer Monitoring
  - Virus Protection
  - Physical Security
  - Encryption
- **Violations of Policy**
  - Procedures for Reporting Violations
  - Penalties for Violations
- **Policy Review and Modification**
  - Scheduled Review of Policy and Procedures for Modification
- **Limitations of Liability**
  - Statements of Liability or Disclaimers

Example: NUS Data Management Policy

NUS DATA MANAGEMENT POLICY

Policy Information	
Category	Governance/Administrative/Operational
Department Responsible	NUS Information Technology (NUS IT)
Contact	Email: dmp@nus.edu.sg
Governance (approved by)	Data Governance and Management Steering Committee (DGMSC)
Audience (applies to)	All users of University Data including: • NUS Faculty and Staff • Part-time Teaching Staff • Contingent (casual/temporary) Staff • NUS and Non-NUS Student assistants, interns, helpers or volunteers (e.g. in departments, NUSSU, clubs and societies, halls and residences) • Volunteers • Contractors, vendors, temporary workers
Brief Purpose	Defines general principles to govern the appropriate collection, use, maintenance, disclosure, disposal and protection of University Data
Initial Version	Version 1.6 – 15 May 2007
Current Version	Version 3.0 – 1 May 2020

Example: NUS Data Management Policy

1. PURPOSE

1.1 The NUS Data Management Policy ("DMP") governs the collection, use, maintenance, disclosure, disposal and protection of University Data and defines the general principles to safeguard University Data.

The six general principles are:

(i) Shared Responsibility through Data Stewardship and Usage
(ii) Confidentiality through Data Classification
(iii) Single Source of Truth through Data Collection and Storage
(iv) Need To Know through Data Sharing and Disclosure
(v) Need To Keep through Data Retention and Disposal
(vi) Security through Data Protection

Single source of truth is important for access control

1.2 Users must adhere to the DMP and use University Data only for the University's purposes to advance its interests. A secure, reliable and accessible University Data source is a valuable asset that will enable the University to make effective decisions to meet the University's education and research objectives as well as comply with the law.

1.3 The DMP serves as an overarching policy for all data management-related documents and activities in the University. As such, all data management-related policies, standards, procedures and guidelines must be aligned with the DMP.

2. DEFINITIONS AND SCOPE

2.1 Please refer to **Appendix A** for all Definitions referenced in this DMP.

2.2 University Data refers to any data or information created, collected, processed, derived or used in any form or medium by the University and its representatives, regardless of where or how it is stored, its mode of transmission, who is using it, or, from where or how its access is gained.

University Data includes both electronic and non-electronic forms of data.

It includes Administrative Data and Research Data (both of which include Personal Data and Analytics Data).

It excludes Teaching and Instructional Materials.

Case: NUS Email Usage Policy #1

5.4 Email

Email is used frequently for correspondence internally and externally for teaching, research, learning, administration or otherwise carry out the functions and purposes of the University.

(i) Users shall not email or transmit defamatory, threatening or abusive messages or any messages that may be reasonably construed as such.

(ii) Users shall not send annoying, abusive or unwanted messages to others.

(iii) Users shall not send unsolicited mass emails within or external to the University, except for purposes specific to the functions and purposes of the University, or which have been approved by a Dean or Director or University representative with equal or higher authority, and in accordance with the requirements of law.

(iv) Users shall not forward messages containing general appeals or warnings like 'virus warnings', 'request for help', by mass mail or otherwise. Users should instead send these messages to the University's NUS IT's helpdesk for verification.

(v) Users shall not forge the identity of or impersonate another person in an email.

(vi) Users shall not knowingly transmit by email any harmful or malicious content (e.g. viruses) or any other content or material that may otherwise violate the civil and criminal laws of Singapore.

(vii) Users shall not misuse mailing lists to flood an individual, group or the email system with numerous or large emails.

Case: NUS Email Usage Policy #2

5.5 Staff and Contingent Worker Email

(i) Staff and Contingent Workers may use their University Assigned Email Accounts (as defined in the Guidelines for Acceptable Use Policy for NUS IT Resources) for incidental personal purposes provided that such use does not:

(a) interfere with the University's operations;
(b) interfere with the staff's employment or other obligations to the University; or
(c) burden the University with noticeable costs.

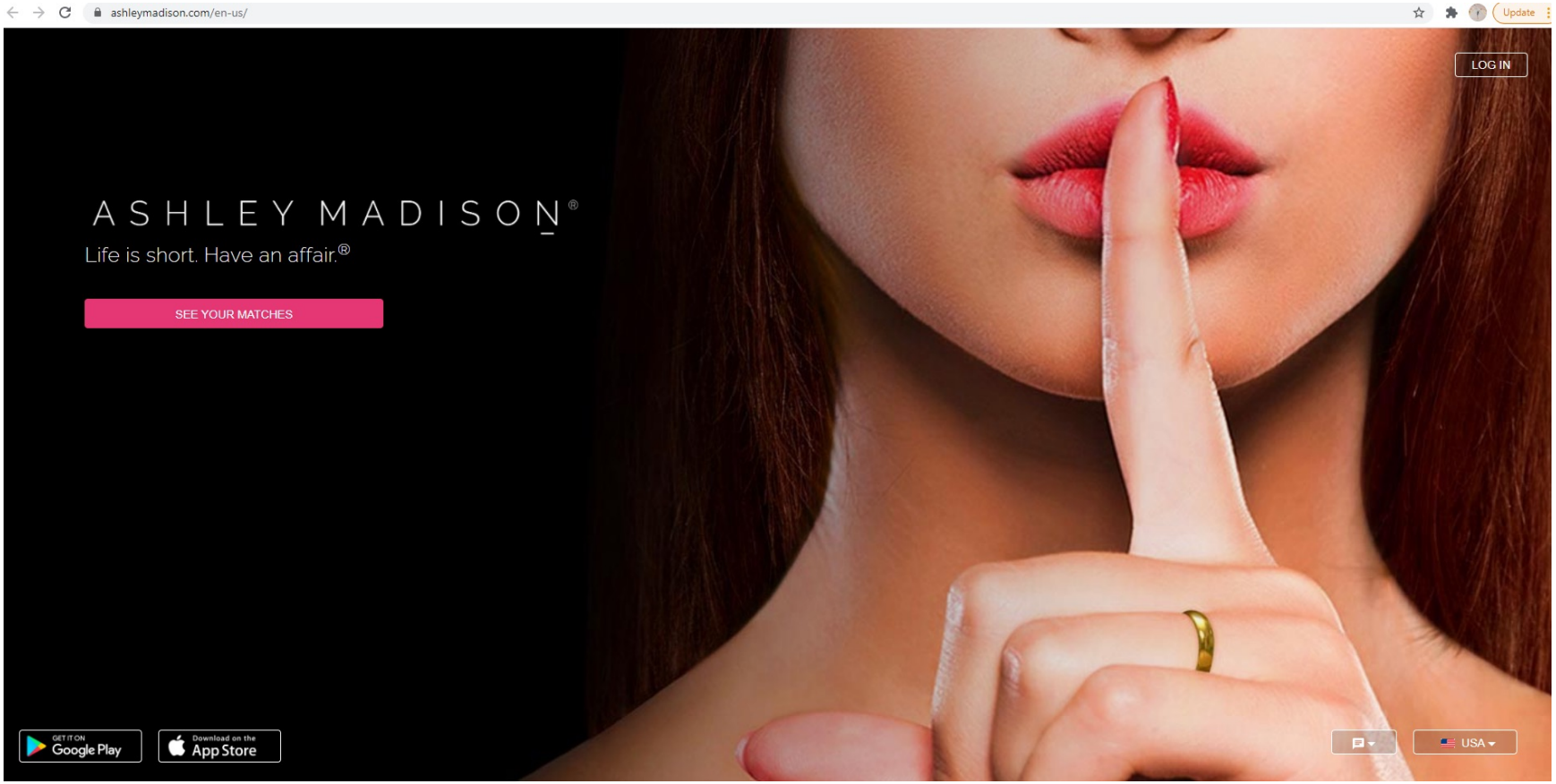
(ii) All Executive and Professional staff, Non-academic staff and Academic Appointment Holder (as defined in Appendix A), shall always use their University Assigned Email Accounts for official correspondence. Staff will compromise the

NUS INTERNAL

---

privacy and confidentiality of University data by not using their University Assigned Email Account or redirecting the email message from their University Assigned Email Account.

Case: Ashley-Madison Data Breach 2015



Case: Ashley-Madison Data Breach 2015

ASHLEY MADISON HACK TIMELINE: KEY EVENTS IN THE ASHLEY MADISON DATA BREACH STORY

Source: https://digitalguardian.com/blog/timeline-ashley-madison-hack

AVID LIFE MEDIA EMPLOYEES GET 'THUNDERSTRUCK'

July 12, 2015: Avid Life Media (Ashley Madison's parent firm) employees log in to find a message from Impact Team threatening to release company and customer data unless the Ashley Madison and Established Men websites are shut down. Impact Team's ransom message is accompanied by the AC/DC song "Thunderstruck."

IMPACT TEAM ANNOUNCES HACK OF ASHLEY MADISON

July 19, 2015: Impact Team publishes their warning message on Pastebin, this time setting a 30 day window for Avid Life Media to shut down the sites before the information is released. The warning is followed by an article from security journalist Brian Krebs announcing the Ashley Madison data breach.

AVID LIFE MEDIA RESPONDS

July 20, 2015: Avid Life Media issues two statements acknowledging "an attempt by an unauthorized party to gain access to our systems" and announcing a joint investigation conducted by Ashley Madison, law enforcement, and the cybersecurity service provider Cycura.

IMPACT TEAM RELEASES TWO ASHLEY MADISON USER NAMES

July 22, 2015: Impact Team releases the names and information of two Ashley Madison users - a man from Brockton, MA and a man from Ontario, Canada - in the first data leak to come from the hack.

'TIME'S UP' FOR ASHLEY MADISON: THE FIRST DATA DUMP

August 18, 2015: Impact Team's 30 day window expires, but Ashley Madison and Established Men are still online. In a Pastebin post titled "TIME'S UP," Impact Team publishes the first major Ashley Madison user data dump, a torrent file containing nearly 10gb of user email addresses. Media outlets and researchers alike scramble to analyze and validate the data.

ANOTHER STATEMENT FROM AVID LIFE MEDIA

August 18, 2015: Following the first data dump, Avid Life Media issues another statement on the hack detailing their investigation and asking for information on the incident.

ASHLEY MADISON USER EMAILS PUBLISHED BY CATEGORY

August 18, 2015: A categorical breakdown of the email addresses disclosed in the first data dump is posted to Pastebin, revealing many government, military, and corporate addresses that were used to sign up for Ashley Madison accounts.

FIRST DATA DUMP CONFIRMED REAL

August 18-19, 2015: After a nearly day-long media frenzy met with much speculation over the validity of the leaked data, Brian Krebs discloses that numerous Ashley Madison account holders have confirmed that their information was published.

ASHLEY MADISON SEARCH WEBSITES APPEAR

August 19-20, 2015: As researchers continue to sift through the first data dump, search websites pop up that let users search to see if their email addresses were leaked.

System-Specific Security Policy (SysSPs)

What are SysSPs?

- SysSPs:
  - Organizational policies that often function as standards or procedures to be used when configuring or maintaining systems.
    - E.g., to configure and operate a network firewall

- Two general kinds of SysSPs:
  - Managerial Guidance SysSPs
    - To guide the implementation and configuration of technology
  - Technical Specification SysSPs
    - System administrators directions on implementing managerial policy
    - Each type of equipment has its own type of policies
    - Two general methods of implementing such technical controls:
      - Access control lists
      - Configuration rules

What are SysSPs?

- Access control lists
  - Include the user access lists, matrices, and capability tables that govern the rights and privileges
  - In general ACLs regulate:
    - *Who* can use the system
    - *What* authorized users can access
    - *When* authorized users can access the system
    - *Where* authorized users can access the system from
    - *How* authorized users can access the system
- Configuration rules
  - Configuration rules are instructional codes that guide the execution of the system when information is passing through it

Main challenges with system level policies and management

What are SysSPs?

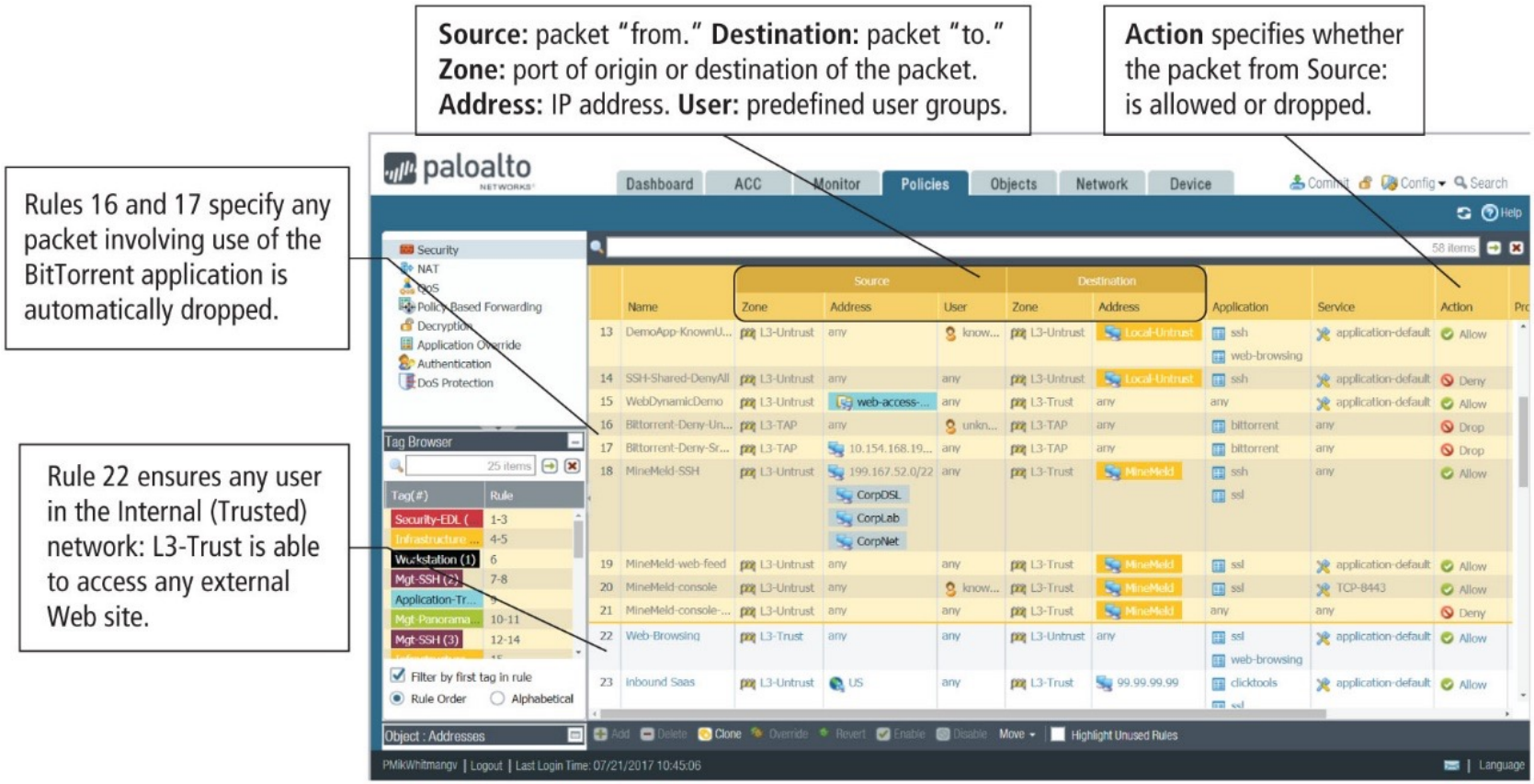


Figure 4-7 Sample Palo Alto firewall configuration rules

Source: Palo Alto Software, Inc.

Guidelines for Effective Policy Development and Implementation

Roles involved in Policy Development and Implementation

- Chief information security officer (CISO)
- Cybersecurity steering committee
- Compliance officer
- Privacy officer
- Internal audit
- Incident response team
- Data owners
- Data custodians
- Data users
- Etc.

risk officer

Guidelines for Effective Policy

- For policies to be effective, they must be properly:
  1. Developed using industry-accepted practices, and formally approved by management
  2. Distributed using all appropriate methods
  3. Read by all employees
  4. Understood by all employees
  5. Formally agreed to by act or affirmation
  6. Uniformly applied and enforced

Policy Development and Implementation Using the SecSDLC

- A policy development or redevelopment project should be
  - Well planned
  - Properly funded
  - Aggressively managed to ensure that it is completed on time and budget
- Use adaptation of SecSDLC for complete policy life-cycle

1. Investigation Phase

- The policy development team should attain:
  - Support from senior management
  - Support and active involvement of IT management, specifically the CIO
  - Clear articulation of goals
  - Participation of the correct individuals from the communities of interest affected by the policies
    - Assign a project champion with sufficient stature and prestige
    - Acquire a capable project manager
  - A detailed outline of the scope of the policy development project and sound estimates for the cost and scheduling of the project

2. Analysis Phase

- The Analysis phase should include the following activities:
  - A new or recent risk assessment or IT audit documenting the current InfoSec needs of the organization
  - The gathering of key reference materials—including any existing policies

- Determine the fundamental policy philosophy
  - "Whitelist" approach
    - "That which is not permitted is prohibited"
  - "Blacklist" approach
    - "That which is not prohibited is permitted"

NUS uses an blacklist approach

3. Design Phase

- The first task in the design phase is the *drafting* of the actual policy document
- There are a number of references and resources available
  - The Web
  - Government Sites
  - Professional Literature
  - Peer networks
  - Professional Consultants
- Next, the development team or committee reviews the work makes recommendations about its revision
- Once the committee approves the document, it goes to the approving manager or executive for sign-off

4. Implementation Phase

- The team must create a plan to *distribute* and verify the distribution of the policies
- Members of the organization must explicitly acknowledge that they have received and read the policy (compliance)
- The simplest way
  - Attach a cover sheet that states "I have received, read, understood, and agreed to this policy"
  - The employee's signature and date provide a paper trail of his or her receipt of the policy
- A stronger mechanism
  - A compliance assessment

5. Maintenance Phase

- The policy development team monitors, maintains, and modifies the policy
- The policy should have a built-in mechanism via which users can report problems with the policy
  - Preferably anonymously

this is to help CIIO owners to check and review their policies

- For CII 1 year
- For normal 5 years

Next Week

- Developing InfoSec Program
  - Chapter 5