# IT 6823 LM 4. Information Security Policy & Access Control

# Learning Material

**Note**: The learning material is composed of a list of web links, videos, and other materials screened and/or created by the instructor. The material is organized by student outcomes. Essential information is included in this document and students are recommended to go to the links to learn more about a specific topic.

## Overview

Information security policy (ISP) provides a set of guidelines on how individuals can work with the IT assets. This module covers the basic principles of ISP and give a general introduction on Identity and Access Management which is major part of ISP.

ISP is a part of Protect function in the NITS security framework. The result of risk assessment, which is covered in LM3, can used as inputs for creating effective ISP.

## Student Learning Outcomes

* **Define information security policy**

“Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information”. Source: <https://csrc.nist.gov/glossary/term/information_security_policy>

* **Explain the main components of information security policy framework**



1) Purposes of ISP:

* + Create an overall approach to information security.
	+ Detect and preempt information security breaches such as misuse of networks, data, applications, and computer systems.
	+ Maintain the reputation of the organization and uphold ethical and legal responsibilities.
	+ Respect customer rights, including how to react to inquiries and complaints about non-compliance.

Source: <https://www.exabeam.com/information-security/information-security-policy/>

2). Audience: Define the audience to whom the information security policy applies. You may also specify which audiences are out of the scope of the policy (for example, staff in another business unit which manages security separately may not be in the scope of the policy).

3.) Information security objectives: Guide your management team to agree on well-defined objectives for strategy and security. Information security focuses on three main objectives: C.I.A.

4). Authority and access control policy

* Hierarchical pattern—a senior manager may have the authority to decide what data can be shared and with whom. The security policy may have different terms for a senior manager vs. a junior employee. The policy should outline the level of authority over data and IT systems for each organizational role.
* Network security policy—users are only able to access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, or tokens. You should monitor all systems and record all login attempts.

5). Data classification

The policy should classify data into categories, which may include “top secret”, “secret”, “confidential” and “public”. Your objective in classifying data is: to ensure that sensitive data cannot be accessed by individuals with lower clearance levels. To protect highly important data and avoid needless security measures for unimportant data.

6). Data support and operations

Data protection regulations—systems that store personal data, or other sensitive data, must be protected according to organizational standards, best practices, industry compliance standards and relevant regulations. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection. Data backup—encrypt data backup according to industry best practices. Securely store backup media, or move backup to secure cloud storage. Movement of data—only transfer data via secure protocols. Encrypt any information copied to portable devices or transmitted across a public network.

7). Security awareness and behavior

Share IT security policies with your staff. Conduct training sessions to inform employees of your security procedures and mechanisms, including data protection measures, access protection measures, and sensitive data classification.

8). Responsibilities, rights, and duties of personnel

Appoint staff to carry out user access reviews, education, change management, incident management, implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy.

**Source**: <https://www.exabeam.com/information-security/information-security-policy/>

**Examples of security policy:** <https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html>

* **Discuss different types of access control**

Be able to explain different type of access control and pros and cons of each.

1. Discretionary Access Control (DAC)

An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability. Source: <https://csrc.nist.gov/glossary/term/discretionary_access_control>

1. Mandatory access control (MAC)

A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. Mandatory Access Control is a type of nondiscretionary access control. Source: <https://csrc.nist.gov/glossary/term/mandatory_access_control>

1. Role-Based Access Control (RBAC)

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. Source: <https://csrc.nist.gov/glossary/term/role_based_access_control>

1. Rule-Based Access Control

Not to be confused with the other “RBAC,” rule-based access control is commonly used as an add-on to the other types of access control. In addition to whatever type of access control you choose, rule-based access control can change the permissions based on a specific set of rules created by the administrator.

Source: <https://www.fourwallssecurity.com.au/blog/4-types-of-access-control>

* **Describe the basics of Bell-LaPadula Model**

Focus on access matrix, access privileges, security clearance level and restrictions

Source: <https://blog.finjan.com/access-control-systems-a-closer-look-at-the-bell-lapadula-model/>

* **Explain ACL and be proficient in change permissions in major OS**
1. ACL definition: “A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object”. Source: <https://csrc.nist.gov/glossary/term/access_control_list>
2. ACL in different OS: <https://en.wikipedia.org/wiki/Access-control_list#Active_Directory_ACLs>
3. File permission for Windows OS (don’t need to know a lot of details, but need to know how to get to the GUI interface or what command to use): a) GUI: <https://www.laptopmag.com/articles/take-ownership-folder-windows-10-using-file-explorer> b) <https://www.iperiusbackup.net/en/how-to-set-reset-ntfs-permissions-file-folder-icacls/>
4. File permission in Unix like (Unix, Mac OS, Linux): <https://www.peachpit.com/articles/article.aspx?p=1403238&seqNum=7>