

***Security and Policy in University Libraries: Ahmed Orwa Library at Emir
Abdelkader University of Islamic Sciences***

Saidi ibtissam

University of Abdelhamid Mehri, Constantine 02 (Algeria). Ibtissam.saidi@univ-constantine2.dz

Received: 13/11/2024

Accepted: 10/02/2025

Abstract:

The increasing security risks to institutions and their information systems have necessarily led to attention to their protection mechanisms. The current study attempts to shed light on the necessity of providing a safe and reliable infrastructure in university libraries to provide electronic services, and directs attention to the need to develop policies and strategies that ensure the security of the library service and the user at the same time ; Where the rules, laws and controls that are applied when dealing with information and related technologies within the library should be available.

The study also aims to verify the existence of such policies in Ahmed Orwa library of Emir Abd El kader University of Islamic Sciences, And the most important protected elements, as it aims to clarify the most important methods adopted to secure digital systems .The study used the Case study method approach and the interview as a data collection tool ; The study concluded that there are some mechanisms to protect the library and its data, such as passwords, antiviruses, etc. However, the results denied the existence of a documented and controlled security policy in the true sense of security policy

Keywords: Security policy , levels of security policies , university libraries

I. INTRODUCTION

Information technology plays a fundamental role in improving processes and procedures within university libraries. It contributes to redirecting functions and enhancing the quality of services provided, raising the effectiveness and efficiency of outputs. If these technologies emerged as alternative solutions to problems in traditional environments such as slow processes and limited spaces, they have also introduced new challenges. Among these challenges are securing and protecting electronic transactions, determining their dimensions, as well as addressing issues of intellectual property protection, copyright, and legal security for electronic information and safeguarding intellectual assets in the networked environment.

This has compelled university libraries to adopt strategies for providing information protection against risks and attacks, safeguarding them from internal and external threats. Through this study, we have attempted to verify the existence of security policies at the level of the Ahmed Aruwa Library at the University of Emir Abd El kader for Islamic Sciences. This aims to ensure the security of library services and user information simultaneously, identifying the key elements covered by protection and examining the methods adopted to secure its automated systems.

Based on this problem, the study aims to answer the following sub-questions:

- What do we mean by security policy, and what are the key characteristics of these policies?
- What are the main components of security policy?
- What are the types and levels of security policy in institutions?
- Does the Ahmed Aruwa Library at the University of Prince Abdul Qadir for Islamic Sciences encompass such policies?
- What are the key elements covered by protection?
- What are the main methods adopted to secure the automated systems of the Ahmed Aruwa Library at the University of Emir Abd El kader for Islamic Sciences?

Study Objectives:

Starting from the research problem, the study seeks to achieve a set of objectives, which can be outlined as follows:

- Define the concept and characteristics of security policy in institutions.
- Highlight the main types of security policies in institutions and outline their levels.

- Examine the experience of the Ahmed Aruwa Library at the University of Emir Abd El kader for Islamic Sciences in providing security policies for the library and identify the elements covered by these policies.
- Identify the main methods adopted to secure the automated systems of the Ahmed Aruwa Library at the University of Emir Abd El kader for Islamic Sciences.

II. Methods and Materials:

The methodology is the path followed by the researcher leading to the discovery of truth through a set of rules that govern the course of action and determine its processes until reaching the specified result. In our study, we have adopted the case study methodology, as it is considered the most suitable for the research topic. The study aims to verify the existence of security policies at the level of the Ahmed Aruwa Library at the University of Emir Abd El kader for Islamic Sciences and identify the key elements covered by protection. Additionally, we aim to examine the main methods adopted to secure the automated systems in the library.

Data Collection Tools:

The success of any research heavily depends on the effective use of appropriate tools to obtain information and data about the phenomenon or problem under study. The researcher must choose the suitable tool, and in our study, we relied on interviews as the primary tool for information collection. These interviews were conducted with the person in charge of the Information Technology unit at the Ahmed Aruwa Library at the University of Emir Abd El kader for Islamic Sciences.

III. The definition of institutional security policy:

It is an official expression intended to denote a set of rules and regulations applied when dealing with information and related technologies within an institution. It outlines what is permissible and what is not allowed. Information security policy is linked to methods of accessing and managing information and its operations. It defines transactions and security solutions for each transaction but does not concern itself with the formulation and engineering of these solutions. Information security policy is reinforced, in the implementation phase, by the information security system, through a set of procedures, tools, and methods collectively referred to as "Security Mechanisms," representing the mechanisms for implementing information security policies. It is also defined as a set of laws, regulations, and guidelines related to how individuals handle information in all its forms, whether electronic, paper-based, or even oral. These laws represent the organization's direction and policy in protecting its information and systems Haut du formulaire (saidi, 2017,p. 99)

The security policy aims to:

- Translating and clarifying security as defined in the rules, principles, and overall objectives of the organization.
- Defining users' responsibilities and duties towards the security of information systems, which include individuals, devices, software, information, etc.

- Stating the procedures to be followed to avoid risks and threats and how to deal with them if they occur.
- Identifying the mechanisms through which the responsibilities and duties for each user are implemented and realized (**Dunham,2020**)

IV. Results and discussion :

1. Responsibility for Information Security at Ahmed Aruwa Library, University of Emir Abd El kader for Islamic Sciences:

Q1: Who is responsible for ensuring the security of information and electronic devices in the library?

Information security is not merely a technical process carried out by specialists alone, but rather the result of collaboration among all employees of a library. Roles and responsibilities are distributed to serve its interests. Therefore, any plan the library formulates regarding information security must encompass comprehensive elements and clauses for all operations and policies related to both technical and human aspects.

Before determining the type and degree of protection, the institution must first take the necessary measures and steps that enable it to impose the required protection. This involves defining responsibilities and duties. The senior management of the University of of Emir Abd El kader is responsible for providing security and protection for its various departments and interests. It establishes the general framework for security decisions and identifies direct executive responsibility, often delegated to the Center for Information Systems, Networks, Media, and Distance Education, which is part of the university as a whole. This center collaborates with the IT cells of each department and center, which, in turn, are responsible for implementing security policies, managing systems, maintaining and updating information, and performing preventive backups.

The security of the library and its interests cannot be effective without involving users (employees who use workstations) as they routinely handle data through the permissions granted to them to perform their work without posing a threat to the security of the library's systems and information. Their responsibilities lie in the legitimate use of the system within the limits of their authority.

2. Security Policy at Ahmed Aruwa Library, University of Emir Abd El kader for Islamic Sciences:

Q2: Does the library have a well-defined and documented security policy with clear guidelines and clauses?

Through the interview conducted with the respondent, who is responsible for the Information Technology unit and systems management at Ahmed Aruwa Library, it was revealed that there is no strategic plan or written information security policy at the library level. Despite the significant importance of this document in defining the directions that facilitate the executive mechanisms to ensure information security, and specifying responsibilities and consequences of potential breaches, the absence of a formalized policy

does not negate the existence of some issued decisions or individual instructions from the library director during regular meetings or continuous monitoring of systems.

Additionally, there are daily directives from the person in charge of the IT unit to employees who have workstations and are authorized to access specific system functions.

3. The essential elements of the information security system at Ahmed Aruwa Library, University Emir Abd El kader for Islamic Sciences:

Q3: What are the most critical elements included in and constituting the electronic security system at the library?

An effective security system must encompass all elements related to the information system, including the security of the infrastructure and its component devices with all their accessories. Securing these components is a top priority, and the most important of these components include:

Firstly, Computer Security:

When interviewing the person in charge of the Information Technology unit for Ahmed Aruwa Library at the University Emir Abd El kader for Islamic Sciences, he emphasized that securing computers is a top priority. This is especially crucial given the rapid developments in the world that have impacted advanced technological capabilities, with malicious intent aiming to breach computer systems for theft, information sabotage, or the destruction of computer devices. He added that the unit regularly seeks to update and renew defensive and preventive measures, within the available resources, to protect against any breaches or sabotage.

However, they face challenges due to the swift evolution of computer devices, which has made the development of equipment used in theft and sabotage surpass user capabilities. This necessitates the continuous enhancement of self-capabilities and monitoring technological advancements in computers and communications. This ensures that the responsible framework for the devices can perform maintenance for emergency breakdowns and verify that the devices are not tampered with or manipulated.

Secondly, Data and Information Security:

Through the interview conducted with the person in charge of the Information Technology Cell for the Ahmed Aruwa Library at the University Emir Abd El kader for Islamic Sciences, it becomes evident that there is a high awareness on their part regarding the importance of securing data and information as a crucial component of the library's information security system. The library consistently balances the security measures employed with providing access to information, recognizing that tightening security measures can sometimes restrict usage. The library relies on backup methods and equips each computer with antivirus software at both the library and the Systems and Networks Center, Televised Media and Distant Education Center. Each staff member has their own account and a personal workspace that cannot be exceeded or bypassed except by those authorized to do so.

Third: Security of Used Software

The person responsible for the Information Technology Cell at Ahmed Aroua Library, Emir Abd El kader University for Islamic Sciences, emphasizes the necessity of considering the security of the software used in libraries. Software is a non-material component and a fundamental element for the successful use of the system. It is also a part of computers, and security would be compromised if operating systems and other programs are neglected. Therefore, we always strive to choose computers with operating systems that have security features capable of protecting software, methods for safeguarding passwords, managing the operating system, and communication systems. This includes defining permissions for reading or writing files and attempting to differentiate between those who are allowed access based on set passwords.

Fourthly: Information Transmission Network Security

The person responsible for the Information Technology Cell at Ahmed Aroua Library, Emir Abd El kader University for Islamic Sciences, The library works on establishing protective measures to ensure the security of networks through continuous system checks and by providing dedicated equipment for monitoring. This is implemented at the level of the Systems Center and the networks of information, communication, distance learning, and e-learning affiliated with the university. The library actively monitors internet connections, restricting access to specific sites for users with authorized accounts, subject to university oversight. The operating systems responsible for managing computers exhibit high efficiency and capabilities, enabling them to detect any intrusion into the network through the design of complex security systems.

"Fifth: Library Staff Security

Through the interview conducted with the person in charge of the Information Technology unit at Ahmed Aroua Library, affiliated with Emir Abd El kader University for Islamic Sciences, we gained significant awareness that the individual plays a fundamental and crucial role in the field of information and computer security. The individual has a substantial impact on the performance of computers, both positively and negatively. They are a key factor in protecting computers and information, but at the same time, they can be a negative factor in terms of sabotaging devices and stealing information, whether for personal interests or the interests of others.

The library works on specifying particular qualifications for employees who possess IT skills and a high sense of responsibility to ensure the security of information. Clear instructions are provided to explain the correct and safe ways to handle devices and information, along with procedures to be taken in case of system failures. This is done to minimize the risks that individuals may pose, in addition to implementing protection programs and conducting periodic reviews to audit the personal and behavioral aspects of employees."

Sixth: Security of Electronic Devices and System Surroundings

The person in charge of the IT department at Ahmed Aroua Library, Emir Abd El kader University for Islamic Sciences, emphasizes the importance of giving attention to the sites and buildings housing computer system devices and their accessories. Depending on the nature of

the systems and applications used, precautionary measures are taken to protect and fortify the site against any sabotage or intrusion, safeguarding it from fire, water leakage, and floods. Efforts are made to maintain the power source continuity, determine inspection methods and procedures, verify the identity of individuals entering and exiting the site, and keep a record of it. As for the library's server location, it is secured from all natural and human risks, placed in the manuscripts store (the most secure place in the library). Specifically regarding access to the server location, only authorized personnel are allowed entry."

4. The role of awareness campaigns in ensuring the security of information and its systems at Ahmed Aroua Library:

Q4: Does the library conduct awareness campaigns about the importance of information security and how to maintain it?

The principle of awareness aims to assist employees in learning and understanding information system security. When asked the following question: "Does the library conduct awareness campaigns about the importance of information security and how to maintain it?" The person in charge of the Information Technology Cell at Ahmed Aroua Library, Emir Abd El kader University for Islamic Sciences, affirmed that there are library awareness campaigns that focus on explaining the importance of information security and how to preserve it. This is achieved by educating employees about the significance of databases, which represent years of work, and emphasizing the need to safeguard them. It includes preventing the compromise of colleagues' accounts and avoiding the connection of external devices (such as flash drives, external hard drives, laptops, and electronic tablets) that could introduce viruses and compromise data.

As confirmed by the head of the Information Technology Cell at the library, we always strive to involve all relevant parties in raising awareness about information security, encouraging them to actively participate in preserving and maintaining security. Thus, the principle of awareness becomes crucial in acquiring appropriate knowledge and understanding the practices and procedures for system security as a whole.

5.The Importance of Ethics in Enhancing the Security System at Ahmed Aroua Library:

Q5: Are ethics considered a security barrier against security breaches in the library? Do you believe that ethics can play a crucial role in achieving information system security in the library?

Professional ethics reflect values and behaviors of individuals, regardless of whether they are within their professional work or outside of it. When asked whether ethics can play a crucial role in achieving security within the library, the head of the Information Technology Cell at Ahmed Aroua Library, Emir Abd El kader University for Islamic Sciences, emphasized the significant importance of professional ethics for society as a whole. Human beings are social creatures who engage in various matters and operations within this society. Organizations seek to achieve security by reinforcing a system of work ethics that enhances the cohesion and better interaction among employees. This, in turn, helps improve the employees' ethics and directly influences their dealings with beneficiaries, adding distinction to the university as a whole. Therefore, the university is committed to applying this system of professional ethics to ensure its security and enhance its reputation among other professional

institutions. This involves not leaking or disclosing professional secrets and building a high level of professional trust by entrusting employees with various significant professional tasks

V. Conclusion:

After analyzing the study data aimed at verifying the existence of security policies at the level of Ahmed Aroua Library, Prince Abdul Qadir University for Islamic Sciences, to ensure the security of library services and important elements contributing to achieving this security, as well as user information simultaneously. Identifying the key elements covered by protection and the methods adopted to secure the automated systems, we arrived at the following results:

- The responsibility for information security at Ahmed Aroua Library lies with everyone, starting from the highest authority in the university, through the executives responsible for the executive interests, to the ultimate beneficiaries.
- The library does not have a written security policy and plan that outlines the data and information protection measures in the library.
- The process of information security at the library is carried out through some decisions issued or individual instructions from the library director during regular meetings or continuous monitoring of systems, as well as daily directives from the person in charge of the IT department to employees who have workstations and are authorized to access specific system functions.
- The person in charge of the IT department at Dr. Ahmed Aroua Library is well aware of the importance of data and information security."
- Ahmed Aroua Library adheres to specific standards when acquiring computers, featuring operating systems with security features that can ensure program protection, password storage methods, operating system management, and communication systems, among others.
- Ahmed Aroua Library works on implementing protective measures and ensuring network security through continuous system checks and providing dedicated equipment for monitoring. This is done at the level of the Systems Center and the networks of information, communication, distance learning, and e-learning affiliated with the university, where continuous monitoring of internet connections is carried out.
- The library ensures the physical security of devices against all natural and human risks, especially the server, which is placed in the manuscript store (the safest place in the library). Access to the store is restricted to authorized personnel only.
- Ahmed Aroua Library conducts awareness campaigns focusing on the importance of information security and how to preserve it.

- The library applies a professional ethics system to achieve security goals and enhance and improve its reputation among other professional institutions."

Study Suggestions:

- Increase awareness of the risks facing the library and its information systems, along with available security and rescue methods to overcome these risks.
- Establish a general framework to assist library officials and staff in developing and implementing measures and practices consistent with information security and its systems.
- Define responsibilities and authorities to prevent the spread of responsibility and commitment to the system from top to bottom.
- Provide each user of the information and communication system with their unique access key, distinct from keys of others, and subject the access key to all adopted security policy requirements.
- Implement technical means to record unsuccessful attempts to breach the system, documenting the date and time of occurrence and identifying the terminal unit used for the attempted breach.
- Discuss and analyze all unsuccessful intrusion attempts, taking necessary measures to fortify the system.
- Encrypt and code sensitive information and data.
- Periodically change encryption keys.
- Assign the task of managing encryption keys to two individuals rather than one, utilizing a dual system to prevent an individual from having exclusive control.
- Separate unnecessary communication lines for accessing computer and information systems.
- Limit the distribution of encrypted and sensitive information to a known and licensed number of recipients as needed.
- Restrict the distribution of information to individuals or departments that require it for their specific functions or tasks.

Referrals and references:

- 1- Saidi , salima.(2017). Information Security and Its Systems in the Digital Age.
- 2- 1Dunham .Information Security Policies: Why They Are Important To Your Organization[on line].MAY 5, 2020. [https://linfordco.com/blog/information-security-policies/.\(25/01/2022\)](https://linfordco.com/blog/information-security-policies/.(25/01/2022))