PERINATAL JOURNAL

Original Article

Perinatal Journal 2026; 34(1):932-943

https://doi.org/10.57239/prn.26.03410096

Information security and confidentiality in a wise government: An analytical study

Jamal Awwad Alkharman[1*], Sami Ahmad Mahmoud Alomari[2], Fadiah Sami Ali Khasawneh[3], Mishael Mohammad Al-Raggad[4], Maher Thamer Saleh Mohammed[5], Maher Ail Moh'D Amoush[6], Alaa Fadhil Khalaf[7], Mamoon Suliman Alsmadi[8], Hanan Shaker Hamoud Jassim[9], Mohamed Abouyounes[10]

[1]Assistants Professor in Law, Jadara University Faculty of Law, Law Department
[2]Assistant Prof. In law, Jadara University, Jordan
[3]Dr. Fadiah Sami Ali Khasawneh, Assistant Professor of Political Science, Jadara University, Faculty of Law, Irbid, Jordan
[5]Master's Student, Quranic Exegesis, Samarra University, Faculty of Islamic Sciences, Department of Islamic Theology and Thought, Baghdad, Iraq
[6]Assistant Professor of Administrative Law, Jadara University, Faculty of Law, Irbid-Jordan
[7]Assistant Professor, Private Law, Civil Law, Lecturer at the Faculty of Law, Al-ALBayan Private University
[8]D, Assistant Professor. Faculty of Law, Ajloun National University, Jordan
[9]Lecturer, Doctor, Islamic Law Philosophy, Iraqi University, Faculty of Islamic Sciences, Department of Sharia, Iraq, Baghdad
[10]Associate Professor of Constitutional and Administrative law, Law department, College of Law, University of Business and Technology, Saudi Arabia, Jeddah, Alhamdaniyah

Abstract

Information security and confidentiality in a wise government are fundamental to the stability and success of the state. This includes protecting data and information from leaks and unauthorized access. Potential factors for national security risks include cyber threats, environmental challenges, and political tensions. Enhancing information security builds trust among citizens and investors and supports economic stability. Implementing information security policies enhances the government's ability to address modern challenges and efficiently safeguard the interests of the state. It is also essential to balance security and transparency to ensure good governance. Through this research, it becomes clear that information security and confidentiality in a wise government comprise a set of policies and procedures aimed at protecting and securing sensitive and important government information. This is achieved through the use of advanced data encryption techniques, restricting access to information, and applying strict measures to prevent unauthorized access. Improving the security and confidentiality of information in a wise government depends on a set of recommendations. Policies should be reviewed and updated regularly to keep pace with technological advancements and new threats. Regular training should be provided to employees on how to handle sensitive information and handle it securely. Encryption techniques should be used to protect data during transmission over networks and during storage. Access should be controlled, with specific individuals designated with the right to access certain types of information, and access restricted to maintain its confidentiality.

Keywords: Information security, Wise government, Networks, Data protection

Introduction

Most organizations have has progressed considerably in deliver their service as a result of the recent technological development, which contributed in developing the used means and methods, through this progress, as the organizations were able to improve their services by using modern means of communication, which significantly enhanced its performance, the electronic services provided by government institutions represent a tremendous improvement in online administrative business networks, this is accomplished through immediate business networks within institutions using the Internet, and this allows for improving the services provided to beneficiaries according to several standards that ensure excellence and innovation in operations, in addition to reduce the cost and improve the quality of services, and contributes to improving administrative performance by providing an effective operating environment that reduces time and effort.

In this context, we must shift from the model of traditional institutions to electronic institutions; as the use of technology in organizations increases the accuracy and speed of performance, and reduces the consumption of time and effort. This includes the use of computers and specialized software to carry out the required tasks, and thus contributes to facilitating obtaining services and providing greater effectiveness for the organization. Therefore, there must be systems that maintain the confidentiality and security of information.

Correspondence: Jamal Awwad Alkharman, Assistants Professor in Law, Jadara University Faculty of Law, Law Department, **e-mail:** j.alkharman@jadara.edu.jo, **Received:** December 3, 2025 **Accepted:** January 13, 2026

The security and confidentiality of information are extremely important in any government that seeks sustainability and stability, and wise governments require attention to information security as an essential component to protect national interests and ensure the continuity of government services, as governments must apply policies and procedures to achieve information security and ensure its confidentiality effectively.

Hence this research paper addresses the information security and confidentiality in a wise government.

Research problem

The research problem lies with the increasing adoption of technology and the use of data in wise governments. Issues of security and confidentiality have become a vital problem that requires attention and continuous research, as there are several problems that affect the security and confidentiality of information in a wise government, including advanced cyber threats, as the threats of advanced cyber-attacks targeting institutions have increased. These threats include hacking attacks, malware, and cyber-attacks that are carried out by advanced and varied means. There may be a lack of awareness of security risks among employees, and sometimes governments may face difficulty in keeping pace with rapid technological developments and updating legislation and policies to be in line with requirements of modern security. With increasing the volume of data and the complexity of technology applications in governments, technical challenges may arise in effectively securing and protecting this data. Hence, the research problem lies in the ability of wise governments to apply effective information security strategies and policies to address the challenges and ensure the confidentiality and security of the information they manage.

Research objectives

The research aims to identify the following:

- Definition of information security and its importance.
- Analysis of information security challenges in a wise government.
- Policies and procedures to enhance information security.

Research Methodology:

The researcher adopted the descriptive analytical approach in identifying the information security and confidentiality in wise government, by examining strategies that demonstrate the importance of information security and what guarantees its confidentiality and security.

First chapter

Definition of information security and its importance

First Topic

Information security means protecting data and information transmitted over the Internet from damage, tampering and unauthorized alteration, and from any threat that may be exposed to it, such as unauthorized access, data tampering and unauthorized access. This includes providing the necessary means and methods to protect it from internal and external risks. Information security is an old topic, but the need and demand for it has increased with the spread of the use of the Internet and its adoption in all areas of life. With the expansion of the use of social media networks, there is greater urgency for this type of protection, which means protecting data and information from leakage or unauthorized access. This includes maintaining the confidentiality of information, ensuring its accuracy and completeness, and securing it from damage or loss. It refers to the reassurance of the beneficiaries that the electronic services provided to them are free from errors, dangers, hacking, or doubts among the beneficiaries that their transactions are under threat, or hacking, and maintaining the confidentiality of the beneficiary’s dealings with the institution. (Al-Kasasbeh, I. A. (2014)

The dimension of security means knowing how to deal with beneficiaries with kindness and courtesy, giving them security in their dealings, and that the institution is very careful about individual and financial information. (Al-Riyadi, S. F. S. (2016); Jam et al., 2018)

Security also represents protection from piracy, the institution's use of antiviruses, protection of the used individual information and services provided to beneficiaries from hacking of websites, and notifying customers of the security of all their information with the institution, as well as the security of the electronic service provided to them from hacking (Qazaniya, 2019). Therefore, the institutions that provide E-Banking services entail providing various guarantees for mobile banking services, which include compensation for financial losses due to service errors .(Alsmadi, M. S., & Balas, H. (2025; Moghavvemi et al., 2025).

The Jordanian Cybercrime Law No. (17) of 2023 defined it in Article (2) as follows: "*Information: data that has been processed and has significance*," and the same definition is stated in the Jordanian Cybersecurity Law No. (16) of 2019.

As for the wise governments, information security is one of the main elements to ensure the sustainability and success of government work. Its importance in the wise governments includes:

- Protecting the national interests: Information security contributes to protecting sensitive data and information related to national security and national interests.
- Ensuring political stability and security: Since data and information constitute a vital part of government work, protecting it enhances political stability and public security.
- Building trust among citizens: The success of the government depends on the trust that citizens have. If they know that their information is safe and protected, it strengthens trust between them and the government.
- Compliance with laws and regulations: The government system is obligated to follow legislation and regulations related to the protection of information. This reflects its commitment to providing services in a transparent and reassuring manner.
- Maintaining the confidentiality of decisions and policies: Information security serve to prevent unauthorized leaks and releases of information that may affect government decisions and policies.
- Maintaining the security of government data: This data includes information related to citizens, companies, and national interests. Therefore, they require special protection to prevent unauthorized access.

So, the researcher believes that information security is extremely important in wise governments, as it contributes to preserving national security, building confidence among citizens, and enhancing political and economic stability.

Second topic: The role of information security in maintaining the stability of good governments

Possible causes of national insecurity include the actions of other countries, such as military attacks or cyberattacks, violent non-state groups such as terrorist organizations, organized criminal groups such as drug cartels, as well as the effects of natural disasters such as floods and earthquakes.

Factors that can lead to insecurity include climate change, economic inequality and marginalization, political exclusion, and reliance on military nationalist elements; These factors have multidimensional impacts, including economic security, energy security, environmental security, border security, and food security, and the role of governments in developing security policies within a national security strategy is increasing. For example, since 2017, countries such as Spain, Sweden, the United Kingdom and United States have joined the countries that have taken this measure. Some countries also appoint a National Security Council and a National Security Advisor to serve as an executive body that advises the President of State on matters of national security and strategic interest (Jabber, M. N. (2025)).

Despite the diversity in states' approaches, coercive power and military force remain the dominant features of security strategies. This force includes military capabilities on land and sea, in addition to air, space, cyberspace, and psychological warfare capabilities. These capabilities can be used for national security defense purposes or for offensive purposes. (Al-Shami, Hassan (2023)

Therefore, the information security plays a pivotal role in maintaining the stability of national security and the national economy. The following is an explanation of its impact on maintaining the stability of national security:

- Protecting sensitive data: This includes protecting national security and economic information from leakage and unauthorized access, preventing its use against the national interest.
- Preventing spying and sabotage: Information security protects against spying attempts and cyber-attacks that could target critical state infrastructure and economic institutions.
- Maintaining public trust: When the public knows that sensitive information is well protected, their confidence in the government and economic system increases, which leads to the stability of the country's economy.
- Promoting innovation and investment: Investors and businesses feel secure knowing that their data and business information are protected, which encourages investment and business development.
- Maintaining economic balance: Information security prevents cyber-attacks that can lead to disruption of vital services and economic infrastructure.
- Achieving economic sustainability: With secure information, the government can effectively plan economic policies and strategies to achieve sustainability in economic growth and development.

In general, information security contributes to building a safe and stable environment to maintain the stability of national security and the national economy, which enhances sustainable development and economic sustainability.

Second chapter

Analysis of information security challenges in the wise government

First topic: Cybersecurity threats and their effects on governments

Cybersecurity has become a strategic weapon in the hands of governments and individuals, as cyberwars have become an integral part of the tactics of modern conflicts between countries. Cybersecurity includes protecting the information of computer devices and networks, including the processes and technologies that ensure their safety from any unauthorized access, alteration or unintentional destruction.

The cybersecurity challenges are among the most prominent challenges facing national security in the twenty-first century. The modern concept of security is not limited to military aspects only, but rather includes all threats and challenges that may constitute an obstacle to the digital economy and the flow of knowledge. With the advancement of information and communications technology, the geographical, political and cultural borders between countries have merged, which puts national sovereignty in the face of new challenges. These challenges include hacking official government websites and information espionage operations at the state level. (Talah, L. (2020)

Despite the many ways and methods of electronic protection to maintain information security, there are no universals in this field, such that it cannot be said that a particular method makes it impossible to hack computers or obtain information illegally, which has led the legislator to resort to punitive means to limit Cybercrime and maintaining information security, which requires us to know cybercrime and information and the law’s response to it, as the current Cybercrime Law No. (17) of 2023 was issued to combat cybercrimes that affect information security, as well as Cybersecurity Law No. (16) of 2019.

The Cybersecurity Law has been defined as a system consisting of the interaction of people, data, information systems and programs on information networks, communications systems and associated infrastructure. In this law, the legislator was concerned with organizing and managing efforts towards achieving cybersecurity, and preparing a center called the National Center for Cybersecurity. It has a legal personality, and Article (6) of the Cybersecurity Law states the following: *“A- The Center aims to build, develop and organize an effective cybersecurity system at the national level to protect the Kingdom from cyberspace threats, and to confront them efficiently and effectively in a way that ensures the sustainability of work and the preservation of* *security." National and the safety of people, property and information. B- In order to achieve its objectives, the Center undertakes the following tasks and powers: 1- Preparing cybersecurity strategies, policies and standards, monitoring their implementation, developing the necessary plans and programs for their implementation and submitting them to the Council for approval. 2- Developing and implementing cybersecurity operations, and providing the necessary support and advice to build Cybersecurity operations teams in the public and private sectors, coordinating response efforts and intervening when needed. 3- Determine cybersecurity standards and controls and classify cybersecurity incidents in accordance with instructions issued for this purpose. 4- Granting a license to cybersecurity service providers in accordance with the requirements, conditions, and fees specified in a system issued for this purpose. 5- Exchanging information, activating cooperation and partnerships, and concluding agreements and memorandums of understanding with national, regional and international bodies related to cybersecurity. 6- Develop the necessary programs to build national capabilities and expertise in the field of cybersecurity and enhance awareness of it at the national level. 7- Cooperation and coordination with relevant authorities to enhance cyberspace security. 8- Preparing draft legislation related to cybersecurity in cooperation with the relevant authorities and submitting them to the Council. 9- Continuous assessment of the cybersecurity situation in the Kingdom in cooperation with relevant authorities in the public and private sectors. 10- Identifying critical infrastructure networks and their sustainability requirements. 11- Create a database of cyber threats. 12- Evaluating the security aspects of e-government services. 13- Evaluating and developing cybersecurity incident response teams. 14- Prepare a policy that includes standards for information security and protection. 15- Supporting scientific research in the fields of cybersecurity in cooperation with universities. 16- Conducting cybersecurity exercises and competitions. 17- Preparing the center's draft annual budget, the annual report on its work, and the final financial statements. 18- Preparing quarterly reports on the Kingdom's cybersecurity situation and submitting them to the Council. 19- Any other tasks or powers stipulated in the regulations and instructions issued based on the provisions of this law".*

Cybersecurity threats are attacks and challenges that target digital systems and data, and come from various sources. Here is an explanation of these threats and their effects on governments:

- **Cyberattacks**

This includes attacks aimed at infiltrating government systems and accessing sensitive data. These breaches can leak sensitive government information and expose matters of national security. Cyberattacks also refer to technical intrusions targeting digital systems and computer networks with the aim of gaining unauthorized access and seizing or manipulating information. These hacks can be of a criminal, political, commercial or even psychological nature, and are often a source of serious threats to digital security. Examples of cyber intrusions include: cyber-attacks, hacker intrusions, unauthorized use of digital resources, and cyber espionage. These attacks can target enterprises, governments, financial institutions, and even individuals. Cybersecurity enhancements and awareness of the risks of hacking are essential in maintaining the integrity of information and reducing these threats.

- **Cyber-Attacks and cyber espionage**

Terrorists spy on people, countries, organizations, entities, or international or national institutions. Electronic spying is characterized by the modern method of using information resources and electronic systems brought by technical civilization in the information age. Terrorist spying operations in the information age target three main goals, which are: Military spying, political spying, and economic spying. In the information age and with the presence of modern technological means, the state's borders are invaded by spy satellites and satellite broadcasts. The means of spying have shifted from traditional methods to electronic methods, especially with the emergence of information networks and their global spread, and with the expansion of electronic commerce across The Internet has turned sources of commercial information into targets for economic espionage.

The attempt to intrusion networks and websites by tampering information system hackers (hackers) is not considered terrorism. Their risks are limited and are often limited to tampering with or destroying the contents, which can be overcome by restoring another copy stored in a secure location. The danger lies in espionage operations carried out. It involves terrorist organizations and various intelligence services in order to obtain state secrets and information, and then divulge them to other hostile countries, or exploit them in a way that harms the public interest and the national unity of the state. Terrorists spy on people, countries, organizations, bodies, or international or national institutions. Electronic espionage is characterized by modern way of using information resources and electronic systems brought by technical civilization in the information age, terrorist espionage operations in the information age target three main goals, namely: military espionage, political espionage, and economic espionage. In the information age, and with the presence of modern technological means, the borders of the state It is permissible by spy satellites and satellite broadcasts. The means of espionage have shifted from traditional methods to electronic methods, especially with the emergence of information networks and their spread globally, and with the expansion of electronic commerce through the World Wide Web (Internet), commercial information sources have turned into targets for economic espionage, and even attempting to penetrate networks and websites Electronic data by tampering with information systems (hackers) is not considered terrorism, as their risks are limited and are often limited to tampering or destroying the contents, which can be overcome by restoring another copy stored in a secure location. The danger lies in espionage operations carried out by terrorist organizations and intelligence services. Various methods in order to obtain state secrets and information, then divulge them to other hostile states, or exploit them in a way that harms the public interest and national unity of the state, and includes using technology to spy on governments and steal confidential information. These attacks can be a source of loss of confidentiality and trust in government.

- **Terrorism cyber attacks**

Terrorism cyber-attacks mean the use of digital technology and electronic networks to carry out acts of violence or attacks targeting institutions or individuals for the purpose of achieving political or social goals. These attacks include the use of cyberattacks and hacking into digital systems to disrupt services, steal information, or promote extremist messages. Cyber terrorist attacks pose a serious threat to digital security and the ability of governments and organizations to provide services properly and securely. There are many groups and individuals who use this method to achieve their political or social goals.

- **Threats from organized groups**

Threats from organized groups include activities carried out by organized and structured groups aimed at achieving certain goals, whether political, social, economic or security. These threats include activities such as terrorism, organized crime, smuggling, espionage, cyber threats, cyber-attacks, and drug-related activities. These groups can pose a serious threat to the national security and political and economic stability of countries. Combating these threats requires international cooperation and effective information exchange between governments, international organizations and security agencies.

- **Sharing and disseminating terrorist information through the information network**

If the meeting of terrorists and criminals in a specific place to learn the methods of crime and terrorism and to share opinions, ideas, and information is difficult in reality, then information networks greatly facilitate this process, as several people can meet in multiple places and at a specific time, and make conversations and listen to each other through the information network. They can gather followers and supporters by disseminating their ideas and principles through websites, forums, and electronic dialogue rooms. Although electronic mail (E-mail) has become one of the most widely used means in various sectors, especially the business sector, because it is easier, safer, and faster to deliver messages, However, it is considered one of the greatest means used in electronic terrorism, through the use of e-mail to communicate between terrorists and exchange information among them. Indeed, in many of the terrorist operations that have occurred recently, e-mail was a means of exchanging information and transmitting it between those carrying out the terrorist operations and their planners. Terrorists also exploit e-mail and benefit from it to spread and promote their ideas, and seek to increase their followers and sympathizers through e-mails.

Through the information network, terrorist organizations and groups are able to spread their extremist ideas, advocate their deviant principles, control the conscience of individuals, and exploit their suffering in order to achieve their illegitimate goals that conflict with the interest of society, as terrorists use the global information network (Internet) on a daily basis to spread their destructive ideas and achieve their bad goals, it is possible to highlight their most important uses of the network as follows: (Ibrahim, K. M. (2008)

A. Communication and concealment: Various terrorist groups and organizations use the Global Information Network to communicate and coordinate among themselves, due to the low costs of communication and messaging using the network compared to other means. The network also provides terrorists with a valuable opportunity to communicate and hide, through e-mail, websites, forums, and electronic dialogue rooms. It is possible to place encrypted messages that do not attract attention, without the terrorist being forced to reveal his identity, and they do not leave a clear trace that can be identified.

B. Collecting terrorist information. The information network is characterized by the abundance of information contained in it, and it is considered a comprehensive multi-cultural electronic encyclopedia, diverse sources, and rich in sensitive information that terrorists seek to obtain, such as the locations of nuclear facilities, power generation sources, command, control and communications locations, international flight schedules, and information related to ways to Combating terrorism, and other information that is considered a valuable treasure for terrorists, due to the detailed information it contains supported by images.

C. Planning and coordination of terrorist operations. Terrorist operations are an act of complexity and difficulty, as they require careful planning and comprehensive coordination. The global information network is considered an extremely important means of communication for terrorist groups, as it allows them the freedom to plan accurately and comprehensively coordinate to launch specific terrorist attacks, in a comfortable atmosphere away from the prying eyes of onlookers. This makes it easier for terrorists to arrange their movements and timing their attacks.

D. Obtaining financing. Through the global information network and by using demographic statistical data selected from the personal information that users enter on the information network, and through inquiries and surveys on websites, terrorists identify people with tender feelings and compassionate hearts, and then they are solicited for financial donations. For legal persons to be a front for these terrorists, this is done through e-mail messages or through electronic dialogue forums, in a smart and deceptive manner, so that the donor does not suspect that he will help one of the terrorist organizations.

E. Mobilization and recruitment of terrorists. Terrorist groups and organizations use the global information network to spread and promote the culture of terrorism, and to disseminate the ideas and philosophies that they advocate. They also strive to provide the largest possible number of people willing to adopt their ideas and principles.

F. Cyber terrorist training. Terrorist operations require special training, and training is one of the most important concerns of terrorist organizations. Secret training camps have been established - as some of them appeared in the media, such as Al-Qaeda - but the problem with terrorist training camps is that they are always at risk and can be discovered and raided at any time, so the network Information technology, with its services and features, has become an important means of terrorist training. Some terrorist groups have also produced guides for terrorist operations that include methods of training, planning, implementation, and concealment. These guides can be disseminated through the information network to reach terrorists in various parts of the world

- **Creating terrorist websites**

Terrorists create and design websites on the Internet to spread their misguided ideas, call for their deviant principles, highlight the strength of the terrorist organization, intellectual mobilization and recruitment of new terrorists, give instructions and electronic indoctrination, and provide electronic training by teaching methods and means that help in carrying out attacks. Terrorist attacks. Electronic terrorist websites have been created to explain how to make bombs, explosives, and deadly chemical weapons, to explain ways to hack e-mail, how to hack and destroy websites, access blocked websites, and to teach ways to spread viruses and so on. (Asiri, A. (2006)

- **Destroying websites, electronic data and information systems**

Terrorist organizations launch electronic attacks through information networks, with the intention of destroying websites, electronic data, and information systems, and damaging and destroying the information infrastructure. Terrorist attacks in the information age often target three main goals: military, political, and economic goals. In the age of the information revolution, we find the same three goals, led by the military command and control centers, then utility institutions such as electricity and water institutions, and then come the banks and financial markets, in order to submit to the will of the peoples and international communities.

Destruction here means illegal entry into a primary or secondary connection point connected to the information network through an automated system (Server-PC), or a group of networked systems (Intranet), with the aim of sabotaging the connection point or the system, and there is no technical or organizational means that can be applied. It completely prevents sites from being permanently destroyed or hacked. Technical variables, and the hacker's familiarity with vulnerabilities in applications, most of which were built on the basis of the open design of most parts (Open source), whether in the components of the connection point, in systems, in the network, or in programming, made Preventing intrusions is very difficult, in addition to the fact that there are terrorist organizations whose work and responsibilities include the desire to infiltrate and destroy websites. It is known that institutions have capabilities that individuals do not have, so computer hackers can access confidential and personal information and penetrate privacy. Information is easily confidential, and this is because the amazing development in the world of computers and information networks is accompanied by greater progress in information crimes and ways to commit them, especially since their perpetrators are not ordinary users, but rather may be experts in the field of computers (Al-Baghdadi, F. A. N. (2025).

One of the methods currently used to destroy websites is to pump hundreds of thousands of electronic messages (E-mails) from the destroyer's computer to the targeted site to affect the storage capacity of the site. This huge number of electronic messages creates pressure that ultimately leads to the explosion of the site operating on the network and the dispersal of the data. The information stored on the site is transmitted to the attacker's device, or enables him to freely roam the targeted site easily and obtain all the numbers, information and data he needs regarding the attacked site.

Viruses are also considered one of the most dangerous elements to information networks. A virus is a computer program that causes harm to the information and data system, and is capable of multiplying and spreading, and moving from one device to another. A computer virus is similar to a natural virus in many ways, as it changes the properties of programs just as a natural virus does. By changing the characteristics of infected cells, it reproduces, spreads, and changes its form just like a natural virus. Viruses are of multiple types, and they are graded in terms of the damage they inflict on devices, starting from minor damage to destroying the entire system. The terrorist can use viruses to spread destruction across information networks and electronic systems. It can also It can also be used for hacking and espionage.

The effects of these threats include loss of sensitive data, disruption of government services, undermining political and economic stability, and loss of public confidence in government. Therefore, achieving cybersecurity is crucial to maintaining the stability and security of governments.

Second topic: Cyber-attacks and ways to confront them

Cyberattacks are operations that target digital systems and computer networks with the aim of gaining unauthorized access, seizing or manipulating information. These attacks include computer viruses, malware, phishing, cyberespionage, and cyber intrusions.

To combat cyberattacks, the following steps can be followed:

- Updating software and systems: Systems and software must be updated regularly to ensure that the latest security patches are installed.
- Use security software: Anti-virus and anti-malware software and firewalls should be installed to prevent unauthorized access.
- Staff Awareness: Employees should be trained on how to recognize cyberattacks and what to do in the event of a threat.
- Implement the security policies: It must to develop and implement data and information security policies in the institution.
- Use encryption techniques: Important and sensitive data should be encrypted to prevent unauthorized access.
- Network Monitoring: Network traffic should be monitored to identify any unusual activity that may indicate attacks.
- Emergency procedures: Plans must be developed to deal with cybersecurity incidents and take necessary measures to contain attacks and restore systems.
- Investigation and Reporting: If an attack occurs, an investigation must be conducted to understand how the attack occurred and preventive measures should be applied to prevent its reoccurrence.
- Cooperation with security authorities: Attacks must be reported to the competent authorities and cooperate with them in investigating and prosecuting those responsible.

It should be noted that digital security should be a high priority for organizations and individuals to maintain the integrity of information and data.

Third chapter

Policies and procedures to enhance information security

First topic: Develop and implement strong information security policies

Information security policies are an essential way to keep systems and data secure, whether it is soft or hard copies data. These policies include a set of directives and rules that determine how to deal with sensitive information and protect it from leaking or hacking. In the current digital age, information security policies have become more important than ever before. In addition to applying traditional security policies such as the use of firewalls and anti-virus software, approving policies that control access to data and determining employee powers is extremely important. Policies should also include procedures for dealing with emergency situations and potential risks. Furthermore, work should be done to enhance awareness of the importance of information security among employees and provide appropriate training and workshops. To achieve the success of information security policies, these policies must be consistent with the organization's trends and needs and be fully supported by senior management (Al-Sarhan, M. F.(2025).

Developing and implementing strong information security policies is critical for enterprises and organizations. Here are some key steps to achieve this:

- Analysis of current security: Careful analysis of weaknesses and loopholes in current security must be done to determine needs.
- Develop policies and procedures: Clear information security policies and procedures must be developed and established that include a set of rules and guidelines for data protection.

- Awareness and training: Employees must be educated and trained on best practices for digital security and how to handle sensitive information.
- Verification and Monitoring: Data traffic must be managed and systems monitored to ensure policies are adhered to and to detect any unauthorized activity.
- Access management: Employees must be assigned specific access levels and ensure they have the necessary permissions to perform their tasks.
- Updating technology and software: Systems, software, and hardware must be updated regularly to avoid exploitation of vulnerabilities.
- Response Procedures: Procedures should be in place to handle, investigate, and recover security incidents.
- Compliance with legislation and regulations: You must ensure that policies comply with applicable laws and regulations.
- Continuous evaluation and improvement: There must be ongoing work to evaluate and improve policies and procedures to ensure they are compatible with technological developments and new security threats.

These steps form an essential framework for developing and implementing strong and effective information security policies.

Second topic: Training employees and raising awareness about information security behaviors

Training employees and raising awareness about information security behaviors is a critical part of protecting sensitive data and information in a facility. This training can include a set of important elements:

- Definition of threats: Explaining the types of threats that information may face and how to deal with them, including cyber-attacks, hacks, and electronic fraud.
- Security Practices: Guidance on how to handle sensitive information, such as not sharing passwords, updating security software regularly, and avoiding opening suspicious email attachments.
- Internal Policies: Explanation and clarification of the facility’s internal policies and rules regarding information security, including the rules for using hardware and software.
- Handling Sensitive Data: Guidance on how to handle sensitive information and customer personal data in a safe and responsible manner.
- Reports and Alerts: Guidance on how to report any information security breaches or the discovery of new threats.
- Virtual tests and practical exercises: Organize exercises and simulate intrusions to assess employee response and practice what to do in the event of a security incident.
- Periodic updates: Providing periodic training sessions to update employees on the latest threats and self-defense methods.
- Providing these training courses and workshops can help strengthen a facility's security culture and protect data from modern threats.

Third topic: Using modern technologies to encrypt and protect government information

The use of modern technologies to encrypt and protect government information is crucial to ensuring the confidentiality and integrity of sensitive data. Here are some techniques and practices used in this context:

- Advanced encryption techniques: The use of strong encryption algorithms based on long and complex keys. These technologies are constantly updated to combat new threats.
- Public-Private Key Infrastructure (PKI): Used to confirm user identities and verify data authenticity. PKI relies on private and public keys to achieve digital signature and data encryption.
- Security Certificates (SSL/TLS): Used to secure communications over a network. SSL/TLS allows encryption of data traveling between a website and a user's browser.
- Filtering and monitoring network traffic: Using filtering systems to detect and monitor network traffic to identify any unauthorized activity.
- Two-Factor Authentication: Provide an

additional layer of security when logging in by requiring a code or additional verification process.

- Identity and Access Management (IAM) systems: Defining rights and permissions for users and systems so that information is accessed specifically as needed.
- Threat Intelligence: Analysis of available information to identify and address potential threats.
- Regular updates and security patches: Systems and software must be updated and maintained regularly to plug potential security vulnerabilities.
- Vulnerability assessment and penetration testing: This includes evaluating systems to discover weaknesses and verify their ability to resist attacks.
- Blockchain technology: Providing a way to record information securely and unforgeable.

Therefore, using these technologies in an integrated manner and implementing them correctly contributes significantly to protecting government information and ensuring its confidentiality and integrity.

Findings and recommendations

Information security and confidentiality are vital in wise governments, as they play a crucial role in maintaining stability and national security. By implementing right policies, procedures and effective directives, information security and confidentiality can be achieved in good governments.

Findings

- Information security and confidentiality in wise government is a set of policies and procedures that aim to protect and secure sensitive and important government information. This is done by using advanced data encryption techniques, restricting access to information, and applying strict procedures to prevent unauthorized access.
- There are several important aspects included in the security and confidentiality of information in wise government, protecting sensitive data and using advanced technologies to encrypt information and ensure its authenticity to ensure that it is not tampered with or changed by unauthorized parties, access and use policies, periodic review and checks, responding to security incidents: There are plans and procedures to deal with Emergencies and security breaches if they occur, identity verification and multi-factor access: Systems are implemented to verify the identity of users and enhance access with multiple factors.
- The Jordanian laws, which consists the Cybercrime Law No. (17) of 2023 and the Cybersecurity Law No. (16) of 2019, showed ways to maintain information security, confront information crime, and combat attacks on information security by developing technical and scientific methods.

Recommendations

Improving the security and confidentiality of information in wise government relies on a set of ancient recommendations that remain important today. It is as follows:

- Security policies should be reviewed and updated periodically to ensure they keep pace with technological developments and new threats, identifying who has access to certain types of information and restricting access to maintain its confidentiality.
- The government should benefit from collaborating with others in the security field to share knowledge and improve practices.
- It is necessary to make national efforts to pursue rapid progress in the field of information security in Jordan, given the danger of information that is circulated daily by computer and the necessity of protecting it from penetration.

References

1.Ibrahim, K. M. (2008), Electronic Information Security, Alexandria University House, 1st Edi.

2.Alsmadi, M. S., & Balas, H. (2025). The human rights dimensions of administrative detention. Al-Biruni Journal of Humanities and Social Sciences, 3(12).

https://doi.org/10.64440/BIRUNI/BIR009

3.Al-Riyadi, S. F. S. (2016). The impact of the dimensions of banking service quality on customer satisfaction in the Arab Bank" (A field study in the city of Zarqa). Unpublished master's thesis, Zarqa University, Jordan.

4.Al-Shami, Hassan (2023). National Security: Concept, Types, Strategies and Threats, Al-Hiwar Al-Mutamaddin, No. 5718, published on 2/10/2023, accessed on 9/5/2023. https://www.ahewar.org/debat/show.art.asp?aid=783082.

5.Al-Sarhan, M. F., & Al-Sarhan, N. Q. M. (2025). The Impact of the Implementation of the Principle of Separation of Powers on Achieving Democracy in Contemporary Political Systems: A Comparative Study Between Presidential and Semi-Presidential Systems (Using the Turkish and French Systems as Models). Al-Biruni Journal of Humanities and Social Sciences, 3(11). https://doi.org/10.64440/BIRUNI/BIR225

6.Hial, A. A., Ashour, A. S., Almzaiel, A. J., & Jabbar, N. Q. (2025). Pathochemical and clinical chemistry assessment of biochemical determinants associated with hemorrhagic fever patients under surgical and anesthetic management in Dhi Qar Province, Iraq. Ibn Sina Journal of Medical Science, Health & Pharmacy, 3(11), 8–14. https://doi.org/10.64440/IBNSINA/SINA008

7.Jabber, M. N. (2025). NATO from formation to expansion: A perspective on international relations. Al-Biruni Journal of Humanities and Social Sciences, 3(10). https://doi.org/10.64440/BIRUNI/BIR006

8.Talah, L. (2020), Cyber Threats and Crimes: Their Impact on the National Security of States and Strategies to Combat Them, Milestones for Legal and Political Studies, Volume (4), Issue (2).

9.Asiri, A. (2006), Terrorism and the Internet, Riyadh: Naif Arab University for Security Sciences, 1st Edi.

10.1Al-Kasasbeh, I. A. (2014). The impact of electronic control on the quality of internal services in Islamic banks operating in Jordan. Unpublished master's thesis, Middle East University, Jordan.

11.Alsamydai, J, M,. Sanad, H, M,. ALbairootI, S, A,. (2014), Measuring customers' attitudes toward banking services offered by Iraqi public and private commercial banks, . International Journal of Business Management & Research (IJBMR), 4(2), Apr: 106.

12.Al-Baghdadi, F. A. N. (2025). Interobserver and intraobserver variability in CT scan reporting of liver hydatid cyst staging and location. Ibn Sina Journal of Medical Science, Health & Pharmacy, 3(11), 1–8. https://doi.org/10.64440/IBNSINA/SINA007

13. Moghavvemi, S., Jam, F. A., & Iqbal Khan, T. (2025). The Impact of Motivation, Opportunity, Financial Ability, and Willingness on Resident Support for Tourism Development. Tourism Planning & Development, 22(1), 63-84.

14. Jam, F. A., Singh, S. K. G., Ng, B. K., & Aziz, N. (2018). The interactive effect of uncertainty avoidance cultural values and leadership styles on open service innovation: A look at malaysian healthcare sector. International Journal of Business and Administrative Studies, 4(5), 208.