ENSURING INFORMATION SECURITY IN PUBLIC INSTITUTIONS, PROTECTING CONFIDENTIAL INFORMATION

Xusanboy Odashaliyev Avazbek o'g'li
Andijan state university
Stage 3 student

https://doi.org/10.5281/zenodo.8375243

Keywords: Information security, infrastructure, agency, citizen records, best practices, phishing awareness, cyber threat, secure payment gateways, network architecture.

In a digitized world, Information Security has become an important issue for public authorities. Government organizations entrusted with large amounts of confidential information must take strict measures to protect information from unauthorized access, data corruption, and cyber threats. This article explores the importance of ensuring information security in public bodies and defines the basic strategies for ensuring the protection of confidential information.

Understanding the importance of Information Security:

Information security in public bodies includes protection of information such as confidential documents, citizen records, financial information, and national security information. The consequences of a security breach can be serious, including national security breaches, privacy breaches, loss of public trust, and possible legal consequences. Human error is an important factor in disrupting information security. Government agencies must conduct regular training programs to train employees in advanced safety experiences, including phishing awareness, social engineering tactics, and responsible use of technology. By increasing the security culture, agencies can reduce the risk of accidental data corruption caused by human factors.

Sensitive data protection.

Information security in state bodies, Information Security plays an important role in state bodies, where the protection of confidential information comes first. With confidential documents, citizen records, financial information, and national security information at risk, public authorities must prioritize strict information protection measures. This article explores the importance of information security in public bodies, shows the possible consequences of security breaches, and highlights the need to take active action to ensure data protection. Government agencies must employ robust network security measures to protect their infrastructure and data. This includes the introduction of firewalls, attack detection and prevention systems, and a secure network architecture. Regular updates and patches to network systems and applications should be applied immediately to eliminate vulnerabilities. Encryption: implement powerful encryption protocols to protect sensitive data during quiet (stored data) and transit (data transfer). Encryption ensures that data remains unreadable and unusable even if it is caught without permission or used without permission.

National security:

State bodies are charged with protecting national security information. Disruptions in this area can have serious consequences, including intelligence operations, compromising diplomatic relations, and threatening public security. By prioritizing information security, agencies can prevent unauthorized access to confidential documents and increase their protection against external threats. Ensuring information security in public bodies is important in protecting confidential information, maintaining public trust, and ensuring national security. By implementing a comprehensive information security system, cooperating with other government structures, and becoming aware of emerging technologies, public authorities can significantly reduce the risks posed by cyberattacks. Robust measures of information security not only strengthen the stability of state organizations, but also help to create a safe and reliable digital ecosystem. The protection of confidential information is an important aspect of ensuring information security in public institutions and other organizations. Sensitive information can include personal data, financial records, medical records, confidential documents, and other information that, if compromised, can have serious consequences for individuals or an organization. Some basic secret data protection strategies and best practices: access control: introduce robust access control mechanisms to restrict access to confidential information to authorized personnel only. This involves setting up user accounts with the appropriate privileges and using multi-factor authentication to enhance security. Data classification: categorizing data according to the level of sensitivity and, accordingly, applying different levels of security measures. Not all data requires the same level of protection, and data classification allows for more targeted security measures. Constant security training: train employees and employees in the best practices of information security, including working with confidential information, detecting phishing attempts, and protecting against social engineering attacks. Data loss prevention (DLP): deploy DLP solutions that monitor and prevent unauthorized transmission of confidential data beyond an organization's network or systems. DLP tools also help identify potential security policy violations. Network security: implement firewalls, attack detection and prevention systems (IDS/IPS), and secure network architecture to protect data from unauthorized access and cyberattacks. Routine security checks and assessments: conduct periodic security audits and vulnerability assessments to identify possible vulnerabilities in the system and actively address them. Safe data disposal: set up proper data disposal procedures to ensure that they are safely deleted or destroyed when no longer needed. Event Response Plan: develop an integrated incident response plan to quickly and efficiently address security breaches or data-related incidents. The plan should include measures to prevent, investigate and eliminate security incidents. Vendor and third-party risk management: if the organization shares confidential information with third-party vendors or partners, make sure they have robust security measures and follow the relevant data protection rules. Data backup and recovery: regularly back up confidential data and check the integrity of your backups. This ensures data recovery in the event of data loss due to hardware failures, ransomware attacks, or other incidents.

Data management: develop clear data management policies and guidelines to ensure that information is handled responsibly, and only the necessary personnel have access to confidential information.

By adopting these measures and adhering to advanced information security experiments, public institutions and organizations can significantly reduce the risk of data corruption and protect confidential information from unauthorized access while ensuring the confidentiality and integrity of important information.

Protection of citizen records and Privacy:

Government agencies deal with citizen records containing confidential personal information. Violations in this area can lead to identity theft, fraud and invasion of privacy. To protect citizens ' data and maintain public trust, it is essential for agencies to establish robust security measures such as strict access control, encryption protocols, and secure data storage. Protection of citizens ' data and privacy is very important for public institutions because they work with a lot of confidential personal information. Citizen data storage not only ensures compliance with data protection laws, but also helps maintain public trust in public services. Basic strategies and practices for protecting citizens ' data and Privacy:minimizing data: collect and maintain only the minimum amount of personal information necessary for the legal purposes of the government. Avoid storing unnecessary information to reduce the possible effects of data corruption.

Privacy by design: implement privacy issues from the earliest stages of system and service development. Integration of privacy protection into the design and architecture of government databases and applications.

Secure data storage: use powerful encryption and access controls to protect citizen records stored in databases and repositories. Make sure the confidential information is stored in a safe, controlled environment.

User authentication and authorization: introduce reliable user authentication mechanisms to make sure only authorized employees access citizen records. Use multi-factor authentication for an additional security layer. Routine security checks: conduct frequent security audits and vulnerability assessments to identify weaknesses and weaknesses in the system. Solve any problems identified during these investigations immediately.

Employee training: train government employees regularly on best practices for data protection and Privacy assurance. They are taught the risks associated with the correct work with the records of citizens and incorrect work with personal data. Event Response Plan: we develop an integrated incident response plan to effectively address data breaches or privacy incidents. The plan should include stages of limitation, investigation, notification and Correction. Data access logs and monitoring: implementation of a registration and monitoring system for monitoring access to citizen records. Regularly review access logs to detect suspicious activity or unauthorized access. Anonymization and pseudononymization: anonymization or aliasing of citizen data as much as possible to protect individual identifiers, allowing data analysis and research. Data sharing agreements: when sharing citizen records with other government bodies or third parties, we conclude formal data sharing agreements that define data protection measures and responsibilities. Transparency and communication: be open about the practice of collecting data with citizens, the purpose of using the data and the security measures to protect their records. We provide clear references and channels for solving citizens ' problems with personal immunity. Compliance with data protection regulations: ensuring compliance with relevant data protection regulations such as General Data Protection Regulations (GDPRS) or local data protection laws. Routine Privacy Impact Assessment (PIAs): we can conduct Pias to identify and reduce privacy risks that may be associated with new projects, systems or processes that include citizen data.

Safe data destruction: we define safe and permanent deletion procedures when citizens ' records are not needed by them or when data storage periods expire. By following these strategies and encouraging a strong culture of personal immunity in public institutions, it is possible to protect the rights of citizens ' personal immunity and build trust between citizens and the government.

Ensuring the integrity of financial information:

Public authorities are responsible for managing financial information, including budgets, transactions, and tax records. Violation of financial information can lead to major economic losses, disruption of public services, and loss of confidence in the government's ability to manage public funds. Strict security measures such as secure payment gateways, routine checks, and encryption protocols are necessary to protect financial information from unauthorized access or manipulation.

Information security is essential to protect confidential documents, citizen records, financial information, and national security information in government agencies. Violations in these areas can have dire consequences, including threats to national security, invasion of privacy, loss of public trust, and possible legal consequences. Through the use of strong security measures, government agencies can protect confidential information, maintain public trust and ensure the effective and safe functioning of their activities. The proactive approach to information security is decisive in the landscape of cybersecurity and data corruption, which is always developing.

Government agencies must develop a clearly defined and mandatory security policy. These policies should address data classification, access control, password management, encryption protocols, incident response procedures, and employee responsibility. In order to adapt to emerging threats and changing technologies, it is necessary to regularly review and update these policies.

Ensuring information security in public bodies is important in protecting confidential information, maintaining public trust, and ensuring national security. By implementing a comprehensive information security system, cooperating with other government structures, and becoming aware of emerging technologies, public authorities can significantly reduce the risks posed by cyberattacks. Robust measures of information security not only strengthen the stability of state organizations, but also help to create a safe and reliable digital ecosystem.

References:

1.AXBOROT TEXNOLOGIYALARI: M. ARIPOV, B. BEGALOV, U. BEGIMQULOY, M. MAMARAJABOV. Toshkent Noshir-2009.
2.Kiber xavfsizlik asoslari : S.K.Ganiyev A.A.Ganiyev. Z.T.Xudoykulov
3.Axborot texnologiyalari (A.Abduqodirov, A.Hayitov, R.Shodiyev)
4.Axborot texnologiyalari (M.Aripov, B.Begalov va b.)
5.Axborot tizimlari va texnologiyalari (S.G'ulomov, R.Alimov va b.)
6.Hisoblash matematikasi va dasturlash (A.Abduqodirov, F.Fozilov, T.Umurzoqov)