



State Comptroller of Israel | Local Government Audit
Report | July 2024

Information Systems

Information Security of Collection Systems in Local Authorities



Information Security of Collection Systems in Local Authorities

Background

Rapid technological development has impacted nearly every aspect of individual life and various sectors of the economy, including the public sector, particularly local authorities. Local authorities use digital systems and online websites to manage their affairs and interact with residents online. Some even offer various online services, allowing residents to make payments, especially property taxes (Arnona), and access information and various services via the Internet. Local authorities collect personal information about their residents, such as names, addresses, ID numbers, phone numbers, medical information, welfare data, and payment methods chosen by residents. This obligates local authorities to protect the information they collect and ensure its security. The collection process is carried out through the local authorities' collection systems, managed and operated by the authorities and service providers for the collection system, both with access to the system's data. The collection system of local authorities is a central system through which they collect payments from residents, enabling them to conduct their ongoing activity. As of the end of 2021, the total population across all local authorities in Israel was about 9.4 million, and their self-generated revenues were about NIS 44 billion. In 2023, 13,040 cyber incidents were reported to the National Cyber Directorate. In 2021, the global cost of cyber damage¹ was USD 6 trillion²; in Israel, the annual economic cost is estimated at least NIS 12 billion annually³.

- 1 A cyber event is an occurrence that indicates a potential disruption in the normal operation of a cyber asset, which is likely caused by intentional activity in cyberspace. A cyber event does not necessarily indicate a cyber attack, but there is reasonable ground to assume so.
- 2 According to data from the World Economic Forum:
<https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime>
- 3 According to data from the National Cyber Directorate:
https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_5_2024



Key Figures

13,040

cyber incidents reported to the National Cyber Directorate (Center 119⁴) in 2023

96

cyber incidents occurred in local authorities during the "Iron Swords" war until the end of December 2023

164

cyber events in local authorities were reported to the National Cyber Directorate from January 2021 to October 2023

4

of the examined local authorities; **A, B, E,** and **F** did not allocate a dedicated budget for information security

2

of the examined local authorities; **B** and **E** failed to register their databases in the Database Register as required under the Protection of Privacy Law, 1981

1

of the examined local authorities; **B** did not fill the position of Chief Information Officer (CIO)⁵

5

of the examined local authorities; **B, C, D, E,** and **F** have no cyber insurance

2

the number of examined local authorities where no data restoration was performed by their collection system service provider: **A** and **E**

⁴ Center 119 is a center of the National Cyber Directorate for reporting cyber incidents, manned 24 hours a day by analysts whose role is to identify the type of threat, assess the extent of potential damage, and provide the appropriate response for both citizens and organizations. From the website of the National Cyber Directorate website.

⁵ Chief Digital Technology and Information Officer.



Audit Actions



From May to December 2023, the State Comptroller's Office examined information security in the collection systems of local authorities. The following were audited: professional guidance for local authorities in cyber security; management of collection system databases; information security policies and procedures; a work plan for handling cyber events; ISO 27001 standard⁶ certification; disaster recovery; physical security of collection systems; monitoring and controlling of actions in the collection system; cyber events; user identification and authentication in the collection system; collection system access permissions management; conducting risk assessments; penetration testing; reporting and control over service providers of the collection system.

The audit was conducted in six local authorities: **Or Akiva**, **Rishon LeZion**, **Rahat**, and **Rehovot** municipalities, **Even Yehuda** local authority, and the **Emek Hefer** regional council, as well as the Ministry of the Interior. Supplementary examinations were conducted at the Privacy Protection Authority and the National Cyber Directorate. External service providers for the collection systems of the examined authorities were also reviewed. Due to the sensitivity of the topics examined, the local authorities are referred to in the report by randomly selected alternative names (e.g., Local Authority A).

Key Findings



Professional Guidance for Local Authorities on Cyber Security – the 2022 State Comptroller's audit⁷ noted that the Ministry of the Interior intended to finalize a framework for the continued operation of the sectoral unit, established in 2015⁸, to guide local authorities on cyber security in coordination with the National Cyber Directorate. As of the current audit, conducted at the end of 2023, an outline has not yet been agreed upon between the Ministry of the Interior and the National Cyber Directorate regarding the continued operation of the sectoral unit within the Ministry of the Interior, and the

6 International Organization for Standardization.

7 The State Comptroller Reports on the Audit in Local Government (2022) "Management of an Information System in Local Authorities" p. 1265.

8 Government Decision No. 2443, with regard to government ministries that impose their regulatory powers on entities or activities exposed to cyber threats. The decision determined that the directors-general of these ministries would be required to regulate cybersecurity preparedness within the sector they operate in, through the establishment of sectoral guidance units.



unit has ceased guiding the local authorities sector. Hence, no sectoral unit is in charge of guiding local authorities in preparing for and handling cyber events. This absence of an official body precludes support, guidance, and supervision regarding cyber preparedness, particularly given increased cyberattacks during "The Sword of Iron War" and the evacuation of local authorities in the south and north of Israel, potentially exposing their computer systems to security risks.

Information Security Policies and Procedures – despite the National Cyber Directorate emphasizing the importance of preparing an information and cyber security policy in June 2021⁹, as outlined in ISO 27001, it was found that three of the examined local authorities – **B**, **C**, and **E** – have no such policy. Local authority **C** has drafted one, but its management has not approved it. The other examined local authorities – **A**, **D**, and **F** – have prepared policy. Additionally, local authorities **B** and **E** have not prepared information security procedures as the Privacy Protection Regulations require. The other examined local authorities – **A**, **C**, **D**, and **F** – have prepared information security procedures. The absence of a policy with clear goals and objectives could compromise local authorities' preparedness to deal with information security and privacy protection issues.






Determining the Security Level of Databases – according to the Privacy Protection Regulations, every local authority must define the security level applicable to each database – medium or high. It was found that local authorities **A** and **C** defined the required security level for their collection system databases as high, based on their scope and in line with the Privacy Protection Regulations. Local authority **F** defined the level of security needed as medium. Local authorities **B**, **D**, and **E** failed to define the required security level for their databases based on their scope. They were, therefore, unaware whether their databases required a high level of security, which imposes special security obligations (compared to a medium level of security). It should be noted that local authority **D** registered its collection system database in the Database Registrar; however, it did not know how to define the security level in line with the Privacy Protection Regulations.

Management of Collection System Databases – despite the Privacy Protection Law, 1981, requirements by which anyone managing or holding a database must register it with the Database Registrar, it was found that two of the examined local authorities – **B** and **E** – did not register their collection system databases. The other authorities **A**, **C**, **D**, and **F** – did register their collection system databases in the registrar. Despite the Privacy Protection Regulations (Data Security), 2017, stipulating that a database owner must prepare a "Database Definitions Document," local authorities **B**, **C**, and **E** possess no such document detailed as required by the regulations. Local authorities **A**, **D**, and **F**

9 "The Defense Doctrine – Managing Risk: The Complete Practical Guide to Cyber Defense of the Organization."







prepared a "Database Definitions Document." Local authority **A** "Database Definitions Document" did not include all the required details.

-  **Appointments to Positions** – in local authorities **A** and **E**, the Information Security Officer also serves as CIO of the local authority, which, according to the Privacy Protection Authority, might raise a potential structural conflict of interest. In local authority **B**, the CIO position remains vacant.
-  **Work Plans for Dealing with Cyber Events** – although the National Cyber Directorate's cyber defense doctrine highlights the need for a work plan to contend with cyber events, local authorities **B**, **C**, and **E** lack an annual plan. Despite the benefits of budget-linked plans, it was found that the work plans of local authorities **A** and **F** are not budget-linked. Furthermore, local authorities **A**, **B**, **E**, and **F** lack dedicated budgets for information security. Without a work plan that includes mapping relevant risks and the necessary defensive response, the ability of these authorities to effectively deal with cyber events could be jeopardized. A budget-linked plan ensures the financial resources needed to mitigate risks.
-  **ISO 27001 Certification** – although it is not obligated to obtain ISO 27001 certification, obtaining it can help local authorities assess their compliance with its information security requirements. Local authorities **A**, **B**, **C**, **D**, **E**, and **F** are not certified under ISO 27001. Moreover, the contracts of local authorities **A** and **B** with their collection system service providers did not require the provider to be ISO 27001 certified. However, the tenders of local authorities **C**, **E**, and **F** did include such a requirement.
-  **Disaster Recovery** – according to the cyber defense doctrine, organizations must ensure they can recover from incidents such as site failures, data deletions, or file encryptions. The need for adequate backups to support recovery efforts is particularly emphasized. Moreover, regular recovery drills and defining backup frequency and types are recommended. Local authority **C** included a reporting requirement for conducting backups in its contract with the collection system service provider. However, local authorities **A**, **B**, **E**, and **F** did not include this requirement. Local authorities **C** and **E** included the obligation to report the execution of recovery drills in their service agreements; local authorities **A**, **B**, and **F** did not include any reporting obligation for recovery drills. Additionally, none of the local authorities, **A**, **B**, **C**, **E**, and **F**, received reports from their collection system service providers on executing backups and recoveries, even though some authorities, such as **C** and **E**, demanded such reporting. According to the Cyber Defense Doctrine's controls, the organization should verify the execution of periodic data recovery. Local authorities **B**, **C**, **D**, and **F** conducted periodic exercises of information recovery from the collection system. However, no such exercises were conducted in local authorities **A** and **E**.
-  **Physical Security of the Collection System** – according to the Privacy Protection Regulations, among other things, database owners should include instructions on the physical and environmental security of the database sites in their information security



procedures. Local authorities **B** and **E** have no procedures regarding information security, including physical security. However, local authorities **A**, **C**, **D**, and **F** have procedures addressing the physical security of the database sites as required by the Privacy Protection Regulations. Local authorities **A**, **C**, and **E** have not conducted physical security checks at the collection system service provider's offices since the beginning of the engagement to ensure that their offices, where the information is stored, meet the physical security requirements. Examination of the server room at local authority **D** raised that the local authority did not control nor document entry and exit to the site where the information system is located; the server room includes neither a temperature monitoring system nor an alert for temperature increases; the glass window above the entrance door to the server room allows access or damage to the server room, and flammable objects were stored in the server room.

-  **Monitoring and Controls of Activities in the Collection System** – according to the Privacy Protection Regulations, database owners should document any event that raises concerns about data integrity, unauthorized use, or exceeding authorization. If possible, such documentation should be based on automatic recording. Local authorities **A**, **C**, **E**, and **F** do not monitor the actions performed by system users within the collection system that are recorded in the control mechanism to detect irregular or unauthorized actions.
-  **Local Authorities Reports on Cyber Incidents to the Cyber Directorate** – the audit raised that local authorities **A**, **B**, **D**, **E**, and **F** did not receive requests from the National Cyber Directorate to report cyber incidents that they encountered. Local authority **C** reported that it received such a request. In local authority **A**, two ransom attempts took place; however, the authority failed to report them to the National Cyber Directorate, claiming that it handled the incidents independently.
-  **Cyber Insurance** – covers cyber event expenses and thus highlights its importance in handling such incidents. Apart from local authority **A**, which has cyber insurance coverage of USD 2 million, local authorities **B**, **C**, **D**, **E**, and **F** lack such coverage. As a result, they may have to bear the total costs of managing and recovering from a cyber event, including the rebuilding of all IT infrastructure.
-  **Identification and Authentication of Users in the Collection System** – according to the Privacy Protection Regulations, identification should be based, where possible, on a physical means exclusively controlled by the authorized user. In local authority **F**, access to the collection system is obtained using a password and a verification code from the mobile phone as required by the Privacy Protection Regulations. In local authorities **A**, **C**, and **E**, two-step verification, including a password and a physical means, is not implemented as required by the service provider agreement and the Privacy Protection Regulations. In local authorities **B** and **D**, two-step verification is not implemented as required by the Privacy Protection Regulations, and the requirement was not included in the agreement. The password policy for local authorities **A**, **C**, **E**, and **F** consists of eight characters, and for local authority **B**, seven characters. Both are fewer than the minimum



of 10 characters defined in the National Cyber Directorate controls. In these authorities, the collection system's password policy includes a complex password requirement. However, in the local authority **D** collection system, the password length is four characters, and the password policy does not require a complex password.

Management of Access Permissions for the Collection System – according to the Privacy Protection Regulations, an automatic documentation mechanism must include user identity. Recording users' identities, such as using their actual names rather than generic aliases (e.g., "general employee"), allows for effective control and traceability of actions performed. In the review of users in the collection systems of local authorities **B** and **E**, the actual names of user names were found. However, in local authorities **A**, **C**, **D**, and **F**, generic usernames (such as department names) were found. These usernames do not allow for the proper identification of system users and make it difficult to trace the individual responsible for specific actions. Additionally, despite the National Cyber Directorate's recommendation for an annual review of user roles and access needs, no such review was conducted in local authorities **A**, **D**, and **E** to identify employees or users who had quit or changed roles without blocking their access. Local authorities **B**, **C**, and **F** performed such a review.

Risk Assessments – risk assessment of the collection system identifies the risks to which the local authority is exposed and establishes a plan to prevent or mitigate them. Although the Privacy Protection Regulations require a risk assessment and penetration test, local authority **D**, which independently manages its collection system, did not conduct a risk assessment. The contracts of local authorities **A**, **B**, **E**, and **F** did not include a binding requirement for reporting risk assessments by the collection system service provider. The contract of local authority **C** did include such a requirement. The collection system service providers for local authorities **A**, **B**, **C**, **E**, and **F** conducted risk assessments, but the results were not reported to the audited local authorities.

Penetration Tests – although the Privacy Protection Regulations require conducting a penetration test, it was found that local authority **D**, which independently manages its collection system, did not conduct a penetration test for the collection system. The Cyber Directorate's guidelines specify that database owners, including local authorities, must establish data and cyber protection protocols within their contracts with service providers, including the authority to conduct cyber audits at the provider's site. Local authorities **A**, **B**, **C**, **E**, and **F**, whose collection systems are managed by a service provider, did not include in their contracts the authority to conduct penetration tests on the collection system managed by the service provider. Local authorities **A**, **B**, **E**, and **F** failed to specify in their contracts the service provider's obligation to report the performance and results of penetration tests. It was also found that although the service providers of the collection systems for local authorities **A**, **B**, **C**, **E**, and **F** did perform penetration tests, the results were not reported to the local authorities.

Monitoring and Checks by the Audited Authorities on Information Security Levels at Service Providers – a cross-sectional audit report conducted by the Privacy







Protection Authority in 2021 found that only 21% of local authorities conduct thorough checks to ensure their service providers comply with the regulations. 60% of authorities asked the provider whether they abide by the agreement and regulations without verifying the accuracy of the statement, and 19% of the authorities did not ensure that the provider abides by the agreement and regulations. Local authorities **A**, **B**, **C**, **E**, and **F**, which receive collection system services from service providers, did not monitor the information security level of their service providers.



Work Plans to Contend with Cyber Events – local authority **D** has prepared a budget-linked work plan.







Cyber Insurance – local authority **A** has cyber insurance.

Key Recommendations







-  As a regulator of local authorities, the Ministry of Interior should collaborate with the National Cyber Directorate to designate a body that serves as a sectoral unit for local authorities. This unit shall guide them regarding cyber event preparedness and supervise the implementation of guidelines committed to in the previous audit report.
-  It is recommended that local authorities **B** and **E** form an information security policy and submit it for approval by the local authority's management to draft information security procedures. Additionally, local authority **C** should complete the preparation of its information security policy and submit it for management approval. Local authorities **B** and **E** and all local authorities that have not prepared an information security procedure or whose procedure is incomplete should prepare such a procedure and include all the provisions stipulated by the Privacy Protection Regulations. The local authority's management should also ensure its implementation. Furthermore, it is recommended that the Privacy Protection Authority, as the central regulator, ensure that the security level of databases throughout the economy, particularly in local authorities, complies with the required information security standards under the law and regulations, including Regulation 4 concerning the establishment of an information security procedure.
-  Local authorities **B**, **D**, and **E** should assess the scope of their databases to determine the required security level. If databases require a high-security level, they should comply with the security requirements stipulated in the regulations for this level.
-  Local authorities **B** and **E** should register their collection system databases under the Privacy Protection Law in the Database Registry. Local authorities **B**, **C**, and **E** should prepare a database definition document for their collection system, including all information



required under the Privacy Protection Regulations. Local authority **A** should ensure all required information is included in its database definition document under the Privacy Protection Regulations.

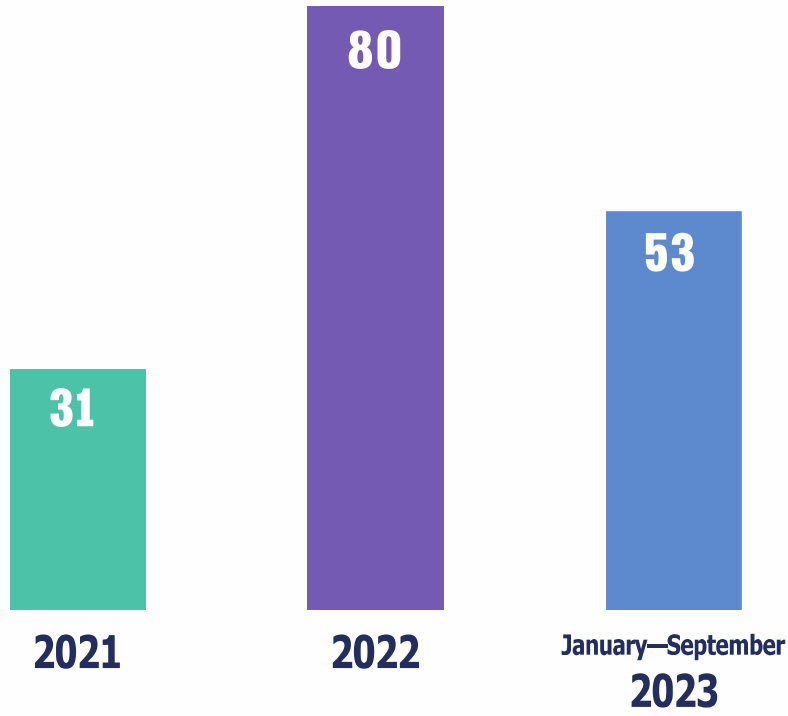
-  Local authorities **A** and **E** should ensure that the roles of Information Security Officer and Chief Information Officer (CIO) are filled by different individuals to comply with the Privacy Protection Regulations. Additionally, it is recommended that local Authority **B** fill the CIO position.
-  It is recommended that Local authorities **A, B, C, E,** and **F** prepare an annual budget-linked work plan to contend with cyber incidents. Additionally, Local authorities **A, B, E,** and **F** should allocate a dedicated budget for information security. While no regulation obligates obtaining the ISO 27001 standard certification, and despite the resources required for its adoption, it is recommended that local authorities pursue the above certification, given the great importance of information security. Furthermore, it is recommended that Local authorities **A** and **B** include a mandatory ISO 27001 certification requirement in tenders and agreements with collection system service providers.
-  In contracts with collection system service providers, it is recommended to include an obligation to report conducting backups and recovery drills. Additionally, local Authorities **A, B, C, E,** and **F** should ensure they receive periodic reports on backups and recovery drills. Local authorities **A** and **E** should verify that the collection system service provider conducts recovery drills at least once a year, under the National Cyber Directorate's recommendations, and that they receive reports on these drills. Furthermore, local authority **D** should conduct an annual recovery drill for its collection system data.
-  Local authorities **B** and **E** should prepare physical information security procedures under the Privacy Protection Regulations. As owners of the collection system databases, local authorities **A, C,** and **E** should ensure that the database meets the physical security requirements. They should examine the physical controls of the service provider to ensure compliance with information security requirements. Local authority **D** should evaluate the security of the site housing its collection system servers, implement access controls, install a temperature monitoring system in the server room (to warn of temperature rise), block the server room wall opening, and remove flammable objects from the room.
-  Local authorities **A, C, E,** and **F** are recommended to regularly monitor activities performed in their collection systems, including identifying unauthorized actions by system users, to detect irregular or unauthorized activities.
-  Until a sectoral unit is established for local authorities serving as an official body in charge of providing professional guidelines to local authorities, it is recommended that the National Cyber Directorate, in collaboration with the Ministry of Interior, guide local authorities to report cyber events to the National Cyber Directorate as soon as possible after they occur. Additionally, it is recommended that all local authorities, including local authority **A,** report any cyber events to the National Cyber Directorate for assistance or to share information about the event.



-  It is recommended that local authorities **B, C, D, E, and F**, which do not have cyber insurance, examine the risk and consider whether they should purchase cyber insurance as a response to it. Additionally, it is recommended that the Cyber Directorate, as the professional guide for the economy in cyber, formulate a policy on cyber insurance.
-  Local authorities **A, B, C, D, and E** should adopt the use of physical means, in addition to a password, to identify users and access the collection system. It is recommended that local authorities **A, B, C, D, E, and F** set a minimum password length of ten characters, according to the controls of the National Cyber Directorate. Additionally, local authority **D** should define a requirement regarding password complexity.
-  Local authorities **A, C, D, and F** should define a username that enables identification of the user performing the actions in the collection system and avoid using generic names that can expose only general information regarding the user's role. Additionally, local authorities **A, D, and E** should conduct a periodic access permission review for collection system users.
-  Local authority **D** (which independently manages its collection system) should determine whether it is required to conduct risk assessments and penetration tests in line with the applicable information security level and relevant regulations. It must carry out the assessments and tests if such a requirement exists. Suppose the security level of local authority **D** is medium rather than high. In that case, it should perform assessments and tests to identify risks and security vulnerabilities for its collection system and formulate a plan to prevent or mitigate them. Local authorities **A, B, E, and F** must ensure that risk assessments are conducted on collection systems managed by service providers. In their contracts with information systems providers, it is recommended that they include a requirement for reporting on the performance and results of risk assessments. Additionally, Local authorities **A, B, C, E, and F** should review the results of risk assessments conducted by the collection system service provider.
-  Local authorities **A, B, C, E, and F** should adhere to the National Cyber Directorate's guidelines by including provisions in their contracts with collection system service providers to authorize penetration tests on the systems managed by the provider. Authorities **A, B, E, and F** should ensure the execution of penetration tests on the collection systems managed by the service providers. In this context, in their contracts with collection system service providers, it is recommended that local authorities include a provision for reporting the execution of penetration tests and their results. It is further recommended that Local Authorities **A, B, C, E, and F** review the outcomes of the penetration tests conducted by the collection system service provider.
-  It is recommended that authorities **A, B, C, E, and F** conduct information security audits at their collection system service providers to ensure they maintain security levels that prevent unauthorized access to the system.



Cyber Events in Local Authorities, January 2021 – September 2023



According to data from the National Cyber Directorate, processed by the State Comptroller's Office.



Summary

Local authorities collect a significant scope of personal information about their residents, which requires protecting and securing this data. These authorities face various risks, including information security vulnerabilities and cyber threats. Cyber attacks on local authorities can cause damage to both the authorities and the general public. It should be noted that following "The Swords of Iron War," the risks of cyber incidents have increased across all entities in the country, including local authorities.

The audit report findings raise deficiencies in implementing the requirements outlined in the Privacy Protection Law, related regulations, and guidelines from the National Cyber Directorate. The above deficiencies might expose local authorities to cyber incidents. Notably, there is a lack of a sectoral unit to guide local authorities on cybersecurity professionally, and there are significant vulnerabilities due to deficiencies in managing the collection system's database. It was also found that the local authorities neither conduct risk assessments nor penetration tests on the collection system nor regularly monitor the service providers who manage their databases. Additionally, they did not receive periodic reports from service providers regarding their compliance with the obligations of the Privacy Protection Regulations.

To reduce local authorities' exposure to cyber threats and ensure the effective use of appropriate information security measures in their collection systems, the Ministry of Interior and the National Cyber Directorate should establish a sectoral unit for local authorities. Additionally, local authorities should address the deficiencies identified in the report to enhance their ability to respond to cyber threats, including conducting security audits on external service providers to assess the adequacy of their security measures.