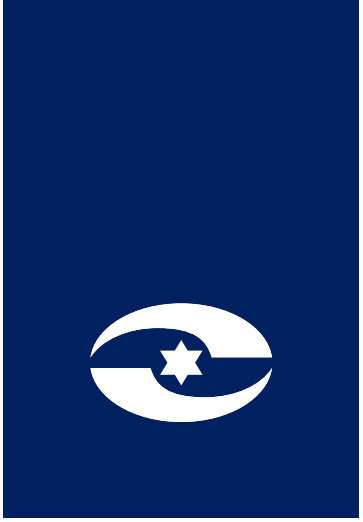


State Comptroller
of Israel

Information Systems Security in the Ministry of Construction and Housing

▪ May 2026 ▪

Information Systems Security in the Ministry of Construction and Housing

Abstract

Background

The Ministry of Construction and Housing (the Ministry of Construction) is responsible for initiating and implementing government policy in the fields of construction and housing. The Ministry focuses on planning and providing housing solutions for the entire population, urban renewal activities, new and rural construction, neighborhood rehabilitation, mortgages, and housing assistance for populations deserving special attention. The Ministry accompanies the entire residential and public-building development process: land identification and planning, land marketing, and infrastructure development. The information that the Ministry of Construction collects, stores, and manages as part of its activities constitutes sensitive information as defined in the Protection of Privacy Law, 5741–1981. The information comprises millions of records, including personal information relating to public housing tenants, recipients of housing assistance, participants in discounted housing programs, and registered contractors. The Ministry is required to protect the confidentiality, integrity, availability, and reliability of this information and must ensure that data are not altered or deleted and are disclosed only to persons authorized by virtue of their position or to those to whom the information pertains.

Key Figures

Dozens

of information systems used by the Ministry of Construction to manage its activities

A certain proportion

of the Ministry's information systems were established many years ago

NIS 6.5 million

The Ministry's information security and cyber budget, constituting approximately 9% of the NIS 74.5 million allocated for IT expenditures in 2025

9

information databases held by the Ministry whose registration in the Database Registry is required, but whose registration has not been completed by the Ministry as required by the Privacy Protection Regulations

130%

The increase in alerts received from the Government SOC (Security Operations Center) regarding the Ministry due to activity suspected of constituting a cyber threat in 2024 (during the "Swords of Iron" War), compared with the alerts received in 2023

43%

Three out of seven cyber-protection indicators that were supposed to be discussed by the Ministry's Cyber Steering Committee in 2025 were not discussed or examined as required

Some

of the external service suppliers using the Ministry's information systems did not undergo periodic reviews to verify that their access authorizations matched their current positions

Audit Actions

Between February and September 2025, the Office of the State Comptroller examined the issue of information systems security and the protection of information privacy at the Ministry of Construction and Housing. Among the matters reviewed were the governance and management of information security and cybersecurity; user and authorization management; the registration of databases; and functional continuity and disaster recovery plans.

Key Findings

Information Security Policy and Budget—Significant changes have occurred in recent years in the field of computing (such as migration to cloud services and the use of artificial intelligence tools in the public sector), as well as technological developments worldwide and advancements in the capabilities of potential attackers. Notwithstanding, the audit found that since the approval of the cyber protection policy in 2020 by the Ministry of Construction's Cyber Steering Committee, it has not been updated, discussed, or reviewed by the Ministry's Cyber Protection Officer every two years, nor has it been updated by the Cyber Steering Committee, contrary to the directive of the Government Cyber Defense Unit (YAHAV). As a result, there is concern that, should risks materialize, the protection against them may not be up to date. In addition, during the years reviewed, the Cyber Steering Committee did not have information regarding the proportion of the budget allocated to information security out of the overall information technology budget, in order to verify that the Ministry was complying with the provisions of the government decision and was assigning sufficient resources to address the security risks facing it.

Mapping and Classification of Information Assets—The audit found that since the Ministry's Cyber Steering Committee first convened in 2020, it has not acted to approve, map, and classify the Ministry's information assets, as required by the YAHAV directive. Although the minutes of the Cyber Steering Committee for the years 2021–2025 noted that asset mapping had been carried out within the Ministry's certification process under ISO 27001 (information security certification by the Standards Institution) and that asset mapping was regularly presented to committee members, the committee itself neither discussed nor reviewed the mapping, nor did it approve it, as required by the YAHAV directive.

In the absence of discussion and examination of the Ministry's information asset mapping, the ability of the Ministry's management to optimally oversee the effectiveness and efficiency of implementation of the cyber protection policy and the suitability of the cyber protection management work plan to the risk level of each system is impaired.

- **Risk Assessments—**Between 2022 and 2024, the Ministry of Construction conducted eight risk assessments. However, despite the obligation under Regulation 5(c) of the Privacy Protection Regulations (Information Security), 5777–2017 (the Privacy Protection Regulations or Information Security Regulations), to discuss the findings of the assessments, formulate a prioritized work plan for addressing and mitigating the risks, and submit it to the Cyber Steering Committee for approval, the committee in practice discussed the findings of only two of the assessments conducted. The remaining assessments were not discussed and the committee did not establish a plan for mitigating the risks identified therein.

- **Penetration Tests—**Despite the obligation of a database owner to conduct penetration tests on database systems at least once every 18 months pursuant to Regulation 5(d) of the Information Security Regulations, during the years 2021–2024 the Ministry of Construction conducted only two application-level penetration tests on two information systems and only one infrastructure penetration test.

  In addition, the findings of the tests conducted by the Ministry were not presented to the Cyber Steering Committee as required. Furthermore, no documents were found indicating that the Ministry had taken any measures to address the risks identified in the tests, including actions to remedy deficiencies and repeat testing to ensure that the deficiencies had been corrected and did not recur.

- **Failure to Ensure Full Performance of Risk Assessments and Penetration Tests Required Under a Supplier Contract—**Although the Ministry's contract with an external company responsible for operating and maintaining information systems stipulated that it must conduct risk assessments for its systems at least once every 18 months and perform penetration tests, the Ministry did not ensure full implementation of the agreement. In practice, the company performed only partial risk assessments and penetration tests required under the contract.

- **Establishment of Cyber Protection Indicators and Compliance with Them—**The audit found that from 2022 until the completion of the audit, the Cyber Steering Committee examined the implementation of the parent cyber-protection indicators only partially and not every six months, as required by the YAHAV directive. For example, at the Cyber Steering Committee meeting held in February 2023, three of the seven approved indicators (approximately 43%) were presented; in January 2024, five of the seven approved indicators (approximately 71%) were presented; and in January 2025, four of the seven approved indicators (approximately 57%) were presented. As a result, the committee's ability to evaluate the effectiveness of the cyber-defense infrastructure and make changes when required was impaired.

- **Access Authorization Management—**The audit found that for more than half of the systems, user authorizations were not reviewed annually as required by the YAHAV directive. It was also found that some active employees and some external service suppliers of the Ministry of Construction did not undergo the periodic review required by the directive. In addition, some users designated as "inactive" in the user file still had valid authorizations according to the authorization review and their access had not been suspended as required.

- **Management of "Privileged" Users (Superusers)—**Superusers possess higher-level privileges than ordinary users, enabling them to make broader changes, manage user lists, and modify infrastructure configurations. The audit found that during the past three years the Ministry of Construction had not conducted the required semi-annual review of superuser authorizations in accordance with the YAHAV directive. The absence of such systematic review increases the risk of excessive authorizations that are not required for actual job performance and is liable to expose information systems to security threats, unrestricted access to sensitive information, and unauthorized actions.

- **Monitoring Access to Databases—**It was found, inter alia, that the information systems within the Ministry of Construction document user access to most databases and allow monitoring thereof. However, unusual activities have not been defined in these systems, and no automated mechanisms exist for generating alerts regarding unusual activities. Consequently, attempts to perform unauthorized actions within the information systems are not monitored through analysis of activity logs as close as possible to real time, and oversight of access to information systems is not optimal and does not comply with requirements.

- **Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP)—**As of the audit completion date, gaps were found regarding the preparation of a business continuity plan that included a disaster recovery plan, as required by the YAHAV directive, including for the purpose of ensuring continued operation of the Ministry's information systems in the event of a disaster.

- **Registration of Databases—**The Ministry of Construction has not regulated the registration of all nine databases that it is required to register under the Privacy Protection Regulations, even though approximately eight years have passed since the regulations entered into force. These databases collectively contain millions of records, including personal information relating to public housing tenants, recipients of housing assistance, participants in discounted housing programs, and registered contractors.

- **Responding to Ransomware Attacks—**The audit found that despite recommendations issued by the National Cyber Directorate and despite ransomware attacks against government institutions, the Ministry of Construction has not yet completed its preparations for a ransomware incident.

Handling of Alerts from the Government SOC—The Ministry of Construction's performance is above average for government ministries (90% of the alerts sent to the Ministry were closed upon receipt of a response, compared with 85% of the alerts in other government ministries).

Key Recommendations

- The Ministry of Construction should discuss the results of the risk assessments and formulate a work plan for addressing and mitigating the identified risks. This plan should be brought before the Cyber Steering Committee for discussion and approval.

- The Ministry of Construction should conduct penetration tests on a broader scale, as required by the Information Security Regulations. In addition, the Ministry should discuss the results of the penetration tests, update the Cyber Steering Committee regarding the risks and threats identified therein, and take action to remedy the deficiencies identified, in accordance with the requirements of the Information Security Regulations. The Cyber Steering Committee should monitor the correction of the deficiencies.

- The Ministry of Construction should ensure that service suppliers fulfill their obligations to conduct risk assessments and penetration tests in accordance with their contractual commitments. It is recommended that the Ministry conduct a lessons-learned process regarding the failure to perform all required assessments and tests and implement oversight and control mechanisms to ensure supplier compliance with the terms of the contracts made with them.

- The Ministry of Construction should conduct authorization reviews across all its systems, as required by the YAHAV directive, and ensure that active authorizations exist for authorized users only .

- The Ministry of Construction should conduct a semi-annual review of superuser privileges, as required by the YAHAV directive .

- The Ministry of Construction should define what constitutes unusual activity and implement automated mechanisms for alerting against it.

- In order to ensure continuity of operations even during emergencies that are liable to affect its information and computing systems, the Ministry should prepare a business continuity plan that includes a disaster recovery plan, based on principles approved by the Cyber Steering Committee .

- The Ministry should regulate the registration of the databases in its possession as required by the regulations, and the Cyber Steering Committee should monitor the registration process and ensure its completion as required.

Summary

The Ministry of Construction is responsible for initiating and implementing government policy in the fields of housing and residential construction. To manage its activities, it uses dozens of information systems containing millions of records, including personal and sensitive information relating, among others things, to public housing tenants, recipients of housing assistance, participants in discounted housing programs, and registered contractors. This information requires a high level of security protection.

This audit identified significant deficiencies in the Ministry of Construction's management of information security and the protection of its systems. Inter alia, it was found that the Ministry's Cyber Steering Committee—which is responsible for formulating information security policy, supervising its implementation, keeping abreast of cyber risks and threats to which the Ministry is exposed, and overseeing cyber-risk management within the Ministry—did not examine or approve the mapping and classification of the Ministry's information assets for the purpose of effective oversight; it devoted only limited attention to the findings of assessments and tests that had been conducted and did not establish a plan for mitigating the risks identified therein; and it failed to ensure implementation of work plans as required by the YAHAV directive. It was also found that the Ministry did not ensure full implementation of risk assessments and penetration tests determined under a contract with an external supplier.

A review of access authorization management revealed that more than half of the systems were not reviewed annually as required by the YAHAV directive and that the Ministry did not maintain an up-to-date list of outsourced employees that would enable it to continuously verify whether former employees were still defined as system users. The Ministry also failed to define unusual activities requiring investigation with respect to access to information systems and did not establish automated alert mechanisms for such activities. Consequently, its oversight of access to its systems is not optimal.

The audit further found that, at the time of its completion, gaps existed regarding a business continuity plan that included a disaster recovery plan for ensuring the continued operation of the Ministry's information systems in the event of such an occurrence.

The Ministry of Construction should take measures to remedy the deficiencies identified in this report in order to improve the protection of the information in its possession and enhance the effectiveness of its activities in this field.