



Report of the State Comptroller of Israel | Cyber and
Information Systems | 2022

Ministry of Education

Special Audit Report – Cyber Protection of Information Systems in the Ministry of Education and of Matriculation Exams and Grades



Special Audit Report – Cyber Protection of Information Systems in the Ministry of Education and of Matriculation Exams and Grades

Background

Most of the information the Ministry of Education collects, keeps, and manages regarding matriculation exams and grades is sensitive information about students and employees, including over 100,000 records. As such, its security must be at the highest level according to the Protection of Privacy Regulations (Data Security), 2017 (Protection of Privacy – Data Security Regulations). The Ministry's duty is to safeguard the information and ensure that it is used only for the purposes for which it was provided or for fulfilling its obligations according to the law. Hence, the Ministry should ensure that the information and data will not be altered or deleted, and will be disclosed only to authorized parties under their role, or to those the information concerns, such as the students or their parents, institutions of higher education and other parties for whom the matriculation certificate and student grades are required.

Another aspect requiring measures to prevent damage to databases is cyber-attacks, the frequency of which is increasing and causing significant and wide-ranging damage. The motives are varied, including the intention to harm the systems themselves and disrupt the regular and ongoing operations of the organization, society, and even the state, for extortion, altering information to garner benefits and reap profits, and as a technological challenge in and of itself.



Key figures

**about
1.39 million**

matriculation exam notebooks evaluated by the Ministry of Education in the 2021 school year (September 2020 – October 2021)

**about
125,000**

12th-grade students took the matriculation exams in 1,299 schools in the 2021 school year

**about
12,000**

exam notebooks suspected of being irregular in the 2021 school year

832

versions of questionnaires formed by the Ministry of Education for 62 subjects in the 2021 school year

**about
2,200**

cyber incidents handled by the National Cyber Directorate in 2021

33%

the increased rate of cyber incidents handled by the National Cyber Directorate in 2021 compared to the previous year

**about NIS
467.6
million**

the Examination Department budget in 2021

**about 5%
instead
of 8%**

the rate of the cyber protection budget allocated by the Ministry of Education from the information technology budget in 2020 (5%) compared to Government Resolution 2443 stipulating 8%

Audit actions







From February 2021 to May 2022, the State Comptroller's Office examined information security in the Ministry of Education and the information security of the central information systems supporting the management and operation of matriculation exam grades and the IT (Information technology) environments in which they operate. The examination was conducted at the Ministry's headquarters, in the Examinations Division, and in the Digital Information Technology Administration, at the Center for Grading Matriculation and Final Exams (the 'Marbad'), which an external company operates. A completion examination was conducted at the Government's Cyber protection Unit (YAHAV) and the Israel Police.

This report was submitted to the Prime Minister on December 6, 2022.



Under the authority vested upon the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], considering the government's reasoning, consulting with the bodies entrusted with the security of defense information, in coordination with the Knesset chairman, and as the subcommittee did not convene, it was decided to publish this report while classifying as confidential parts thereof. These sections will not be submitted before the Knesset or published.

Key findings

-  **Conducting a risk assessment and penetration tests and implementing the annual work plan** – as of October 2021, over three years after the Ministry of Education conducted a comprehensive risk assessment of its selected core systems and a penetration test regarding System A, the ministry did not conduct a comprehensive risk assessment and penetration tests of its core systems as frequently as required by the Protection of Privacy – Data Security Regulations – once every 18 months. Of the seven tasks defined as "critical" or "high" risk level in the Ministry's 2019 work plan and determined to be carried out in 2019, as of October 2021, the Ministry has completed three tasks and has partially addressed the remaining four tasks.
-  **The Ministry of Education's preparedness for disaster recovery** – the Ministry of Education did not perform specific drills for restoring information and for disaster recovery as required by the Government's Cyber protection Unit (YAHAV) guideline "Backing up and restoring information." It also did not perform a drill to restore one of its computer systems completely.
-  **The Ministry of Education's compliance with the obligations promulgated under the Protection of Privacy – Data Security Regulations** – it was raised that three years after the entry into force of the Protection of Privacy – Data Security Regulations (in May 2018), the Ministry compiled the database structure documents, the definitions of the database, and the inventory list for only five (10%) of the 50 databases registered in the Registry of Databases. In the "Students" database definition document, the identity of the information security officer was not updated, and the inventory list is incomplete.
-  **The appointment of a Cyber Protection Officer, convening of a Cyber Steering Committee, and budget allocation for cyber protection** – from the end of 2020 until October 2021, the Ministry of Education did not staff the position of Cyber Protection Officer. The Cyber Steering Committee did not convene at the frequency required – at least once every six months. The Ministry also did not comply with the guideline, by which at least 8% of the information technology budget must be allocated for cyber



protection. In practice, the rate of the dedicated budget allocated for this purpose in 2019 was about 5.66%, and in 2020, it decreased to about 5.06%. It should be noted that the Ministry of Education stated in its response that in June 2022, a Cyber Protection Officer was appointed and that in 2022 (after the audit completion), it convened the Steering Committees for Information and Cyber Security twice.



Information Security on Network A – network A serves all users who are not employees of the Ministry of Education, including schools, teaching staff, students, parents, and suppliers. It is also accessible to Ministry employees according to their needs. Company A provides the Ministry with the network's central infrastructure services. Following are the key findings regarding Network A:

- It was raised that, a specific component and the network and information security equipment, which is under the care of Company A according to the engagement contract, are not directly accessible to the Ministry. The Ministry also does not request the company to periodically report the definitions and rules established for the rest of the network equipment and information security under its control, although, it is required to ensure that the definitions and regulations of the rest of the network equipment and information security meet the requirements in the engagement contract, the Ministry of Education's needs, and the Government's Cyber protection Unit guidelines that apply to it.
- The Ministry of Education did not ask for references documenting how Company A handled its calls, nor did it require it to send a file of the action records (the log file), allowing it to monitor the records documenting the actions performed in the systems.
- System E, which is supposed to allow monitoring of changes in the rules of specific protection components and controlling them, was not implemented on components under the control of Company A.
- The Ministry did not connect Network A to the government SOC¹.



Information Security on Network C – the process of the inspection and evaluation of the exam notebooks used by the examinees to answer the exam questionnaires is managed in Network C. Regarding Network C, the audit raised as follows:

- The network is protected by an outdated version of a specific protection system, which is unsupported by its manufacturer since September 2019. As of November 2021, a specific updated protection system has not yet been fully implemented in Network C.

1 The government command and control center for cyber threats – Security Operation Center (the Government SOC).



- Inconsistencies arose in this network regarding specific components for information security.
- In January 2020, the manufacturer stopped supporting the operating system of certain types of servers that are used, among others, Network C.
- Network C does not have a component that performs a specific control operation at the infrastructure level, as recommended in the guidelines.
- Server A and Server B of Network C are not separated; this allows certain employees access to Server B, even though they should not have such access. A copy of a specific database (DB) is kept on Server A, and it is accessible to authorized users who have been given access to this server. It was raised that those users also have access to a specific database even though they are not authorized to have such access.



Information Security on System D – the files of the scanned exam notebooks and the computerized exam notebooks are loaded onto System D. Access to the system is granted, through the internet, to about 4,000 external evaluators who examine the exam notebooks and enter scores for them. Concerning this system, the audit raised the following:

- The evaluators connect to the system using personal computers that are not managed or hardened by the Ministry of Education and their connection is partially secured.
- The actions performed in System D are registered and documented in the log files, but they are not audited or monitored.
- Six out of eight users whose job was defined in System D under a specific definition received privileges that go beyond their role, not according to the "need to know" principle²; sometimes, there is no unique identification of users or details of the actions performed.
- Files are transferred between System D and the Ministry of Education (or its other suppliers) without being checked whether they contain any risk of harm, even though the regulations require a specific action when transferring information on the public network or the internet. Some files contain sensitive information that is transferred from System D to the Ministry through interfaces that are not sufficiently secure, increasing the risk of sensitive information leakage and damage.
- As part of a particular examination carried out by the State Comptroller's Office on System D, it was raised that the installation of the user side (Client) and the server

2 The "need-to-know principle" – minimizes to the extent possible the parties authorized to be exposed to the particularly sensitive information assets and provides transparency within the Ministry regarding information assets with lower security clearance classification.



side (Server) and the checking of the permissions are not as required by the Government's Cyber protection Unit guidelines.



Information security on System B – system B is used to register the students taking the matriculation exams; About 250 of the schools also use it to enter the students' annual grades (the pre-matriculation grades). Regarding this system, the following was raised:

- 64% of users have not logged into the system for nearly five years – between March 2017 and January 2022; 19% of the users logged into the system about three to five years ago at the latest (in 2017–2019), and only 12% of the users logged into the system in the last year – January 2021 to January 2022. This raises concerns about granting access to the system to parties who do not need them.
- As of September 2021, the Ministry of Education did not scan files in a whitening (anti malware) system before transferring them to Environment B. As of November 2021, the external company did not scan the same files before importing them into Environment A or uploading them in System D.



System G on Network B – the Ministry of Education did not regulate a procedure for the process of updating matriculation grades in System G, the entities involved, those responsible for each step, and the control over the process. Gaps arose in the Ministry of Education's monitoring and control mechanisms. The Ministry also does not perform retrospective audit – it has not regulated a process for receiving a regular periodic report of the actions performed in the system and locating activities suspected of being abnormal. The system also does not allow internal audit in a specific aspect.



Unauthorized distribution of matriculation exams – the audit found seven groups in instant messaging applications operating in the Jewish sector and the Arab sector, where the unauthorized distribution of questionnaires and the solutions to the questionnaires took place. In 2018–2020, the Ministry of Education filed only four complaints at the Israel Police for the offense of "obtaining by fraud" following the unauthorized distribution of matriculation exam questionnaires or answers. It should be noted that in 2020 the Ministry disqualified more than 16,000 exam notebooks due to suspicion of violating the purity of the exams.



Changing the model of the distribution of exams – in 2015, the Ministry established a ministerial team to examine the preparation for the matriculation exams. In 2018, it mapped and analyzed the processes and risks in the Examination Division through an external company. As a result, the Ministry changed the matriculation exam distribution model. Among other things, it purchased and installed hundreds of iron safes in the schools, in which it keeps the matriculation exam questionnaires, allowing it to control its opening time remotely.

Key recommendations

- 💡 It is recommended that the Ministry of Education convene the Cyber Steering Committee twice a year; implement the annual work plan on time; perform risk assessments and penetration tests once every 18 months; allocate at least 8% of the information technology budget to promote cyber protection under Government Resolution 2443 and the Government's Cyber protection Unit's (YAHAV) guidelines.
- 💡 It is recommended that the Ministry of Education require references documenting Company A's handling of its calls and receive monitoring and audit reports, reports of the rules of a specific protection component, and definitions of the equipment for which Company A is responsible. It is further recommended that the Ministry of Education consider implementing measures to monitor the security of the components under the control of Company A, and connect Network A to the government SOC.
- 💡 It is recommended that the Ministry of Education complete the implementation of the updated version of a specific protection component in Network C and upgrade the operating systems of Network C's servers that the manufacturer no longer supports. It is recommended that the Ministry of Education require the companies that operate the Center for Grading Matriculation and Final Exams ('Marbad') on its behalf to integrate the missing information security systems. It is also recommended that the Ministry establish capabilities for specific documentation and control of Network A and set alerts to detect risks of harm to the network.
- 💡 It is recommended that the Ministry of Education perform periodic backup recovery drills and disaster recovery drills; to separate Server A and Server B of System D in certain aspects; and that a specific database is not used on Server A.
- 💡 It is recommended that the Ministry re-examine the evaluators' connection model to System D from personal computers using a partially secure connection; that the Ministry ensure that the companies operating the Center for Grading Matriculation and Final Exams ('Marbad') on its behalf will follow the "need to know" principle and enable access



to information according to the user required information for performing their work only; and that the Ministry improve the monitoring and control capabilities in System D.



It is recommended that the Ministry of Education implement the white system in Network A and Network C. Regarding the transfer of sensitive information between its systems and external systems, the Ministry of Education should improve its protection capabilities against risks potentially causing harm or disruption to its systems and the information therein, under the Protection of Privacy – Data Security Regulations.



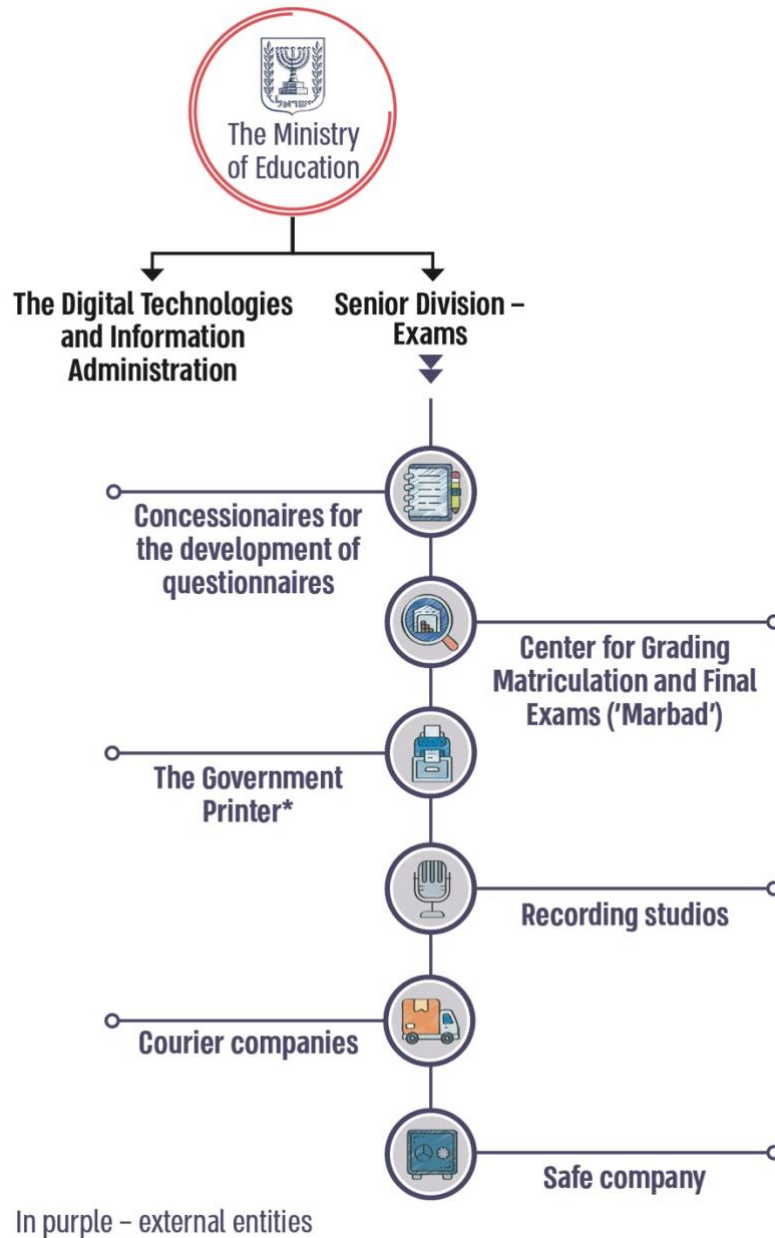
It is recommended that the Ministry of Education examine the list of those authorized to access System B and the permissions granted to them and perform a permission check among System B users, emphasizing changes made to the approvals. It is also recommended to consider implementing an automatic mechanism canceling access to the system of a user who has not logged into it for a period to be defined.



It is recommended that the Ministry of Education and the Israel Police consider tools to contend with the unauthorized distribution of the matriculation exams and the distribution of answers to them before they are over, for example, through monitoring and proactive checks on the various platforms where questionnaires and answers are distributed, including social networks and instant messaging applications.



The key entities involved in the management and operation process of matriculation exams



According to information collected during the audit, and processed by the State Comptroller's Office.

- * The Government Printer is an auxiliary unit in the Ministry of Finance. Its primary role – the execution and production of printing work for the government ministries and auxiliary units through self-production or engagements with external subcontractors.



Summary

The Ministry of Education collects, saves, and manages considerable information about the matriculation exams. This is sensitive information, and its security should be at the highest level. The audit raised several deficiencies in information security – both in the maintaining proper information security governance in the Ministry of Education and in external outsourcing parties, and in the technical areas of implementing information security and cyber protection tools, systems and mechanisms under the Protection of Privacy – Data Security Regulations and the Government's Cyber protection Unit (YAHAV) guidelines.

The findings in the report and the basic problems may endanger the integrity, availability, confidentiality, and reliability of the matriculation exam scores. There is also the concern of harm to the principles of exam purity. The State Comptroller's Office recommends that the Ministry of Education rectify the deficiencies raised in the report, including complying with the schedules established in work plans in information security and cyber protection, improving and increasing the level of information security and cyber protection in all its systems and infrastructures. It is also recommended that the new system managing the matriculation grades, which the Ministry says it is developing, will contend with the findings raised in this report regarding the security of the information of the matriculation exams and matriculation grades.