Report of the State Comptroller of Israel – Cyber and Information Systems | November 2024

Israel Postal Company

Information Systems at the Israel Postal Company and the Postal Bank

Information Systems at the Israel Postal Company and the Postal Bank

Background

The Israel Postal Company is a government company wholly owned by the State of Israel, which provides postal services and operates banking services through its subsidiary – the Postal Bank. As of the end of 2023, the Israel Postal Company and the Israel Postal Bank operate 400 postal units, 650 delivery centers, and about 60 regional postal centers. In 2023, about 11.9 million customers received services from the Company and the Bank.

The Postal Company offers diverse services, including domestic postal services, shipping documents and goods between Israel and abroad, and a network of courier centers distributing for business and private customers across the country.

The Postal Bank serves business customers, government bodies, and the general public. It is government-owned and operates under the supervision of the Ministry of Communications, similar to the Israel Postal Company. Services are offered through about 400 postal branches, including banking teller services. The Postal Bank manages around 510,000 bank accounts, with total deposits of about NIS 4.7 billion. It carries out about 22 million transactions with casual customers annually, and the total number of its customers is about one million.

The Postal Company and Postal Bank utilize various information systems, encompassing operational systems for export and customs, digital services, courier services, banking and retail, headquarters operations, infrastructure and information security, operation and telephony systems.

In April 2023, a cyber-attack on the postal information systems was identified. An examination conducted by the Information Systems Division's information and cyber security teams on April 2, 2023, raised suspicious activity within the postal information systems. On April 5, 2023, an incident response[1] (IR) team from an external cybersecurity firm was engaged. As a precaution, the Company disconnected the postal systems from the Internet. The external firm discovered indicators of unauthorized activity within the organization's systems dating back to July 2022. Despite their efforts, the external company could not identify the attacker, who successfully extracted the user and password database. Consequently, numerous services were rendered inactive, including online payments, vehicle ownership transfers,

1 Incident response to cyber incidents team.

payments to the execution offices, and transfers to HMOs, along with delays in releasing items from abroad. As the work of the external team progressed, services were gradually restored.

Key Figures

NIS 124 million

annual average operating and investment expenses of the Information Systems Division in 2019–2022

55

information systems at the Israel Postal Company. The Postal Bank has 16 additional information systems

48.75%

the decrease rate in the planned investment budget in the Information Systems Division from NIS 64.2 million in 2019 to NIS 32.9 million in 2022

64%

inquiries rate regarding hardware failures out of the total failures inquiries that Shut down end stations in postal units

683

computers were replaced or upgraded out of the 1,850 that required replacing or upgrading to WIN 10

85

of System C[2] permission holders (3% of all permission holders) are not defined in the Human Resources system as active employees in the Company as of January 2024

780

of active permission holders in the network's[3] central management system (13% of all permission holders) are employees who are not included in the list of active employees in the Company's Human Resources system

449

out of 780 active permission holders who are not listed as "active" in the Human Resources system have not logged on to the network's central management system since the beginning of 2024

2 The central system for managing teller processes also serves as the Israel Post cash register for all financial transactions carried out in branches and offices.

3 A dedicated set of tools used for centralized management of computer networks in organizations.

Audit Actions

From June 2023 to March 2024, the State Comptroller's Office Audited the Israel Postal Company and the Postal Bank information systems. The audit was performed at both the Postal Company and the Postal Bank. The audit examined the management and control user permissions at the Postal Company. Additional examinations were conducted at the Ministry of Communications.

Key Findings

- **Connecting the Postal Company's Security Operations Center (SOC) to the Ministry of Communications' Sectoral SOC –** a critical component within the system for securing organizational data and resources is the Security Operations Center (SOC). This center among other roles, monitors unusual activities, assesses potential threats, and provides insights based on investigations following incidents. The Postal Company operates its SOC under the supervision of the Information Systems Division and procures SOC services from a private entity. The audit raised that during 2022–2023, the Ministry of Communications' sectoral unit, which operates a sectoral SOC funded by both the Ministry of Communications and the National Cyber Directorate, made multiple inquiries to the Postal Company regarding connectivity to the Ministry's SOC. However, the Postal Company had not established this connection as of the audit end date. Consequently, the Company is not using the advantages inherent in connecting to the Ministry of Communications SOC, including enhanced external supervision during cyber incidents.

- **Annual and Multi-Annual Work Plans in the Information Systems –** despite a substantial budget for the Information Systems Division at the Postal Company, from about NIS 102 million to NIS 136 million, 17.2% to 19.6% of the Company's total budget (about NIS 102 million out of a total budget of about NIS 592 million in 2022 and about NIS 136 million out of a total budget of about NIS 693 million in 2020), no established procedure exists for managing work plans. Furthermore, in 2019–2023, no multi-annual work plan for information systems was developed. The formulation process for the work plan, as of 2023, does not incorporate departmental alternatives and predominantly relies on a fixed budget. The execution of the work plan lacks monitoring, inhibiting the management's ability to ascertain its status or any adjustments made. Additionally, tracking budget reallocations across tasks is unfeasible, and even the Management of the Information Systems Department lacks transparency regarding allocating working hours per task. It should be noted that in 2024, the Company implemented specialized software for team and project management.

- **Malfunctions in Information Systems at the Postal Company and the Postal Bank –** in 2018, the Information Systems Department presented the need to replace outdated computing equipment in the end stations due to numerous hardware malfunctions. According to the Company's data, from April 1, 2022, to July 21, 2023, system users submitted 46,349 inquiries classified as hardware malfunctions. These inquiries represent the largest category, at about 35% of total inquiries. About 64% of inquiries related to faults resulting in the shutdown of end stations identified hardware issues of 3,306 inquiries out of 5,178 examined. Additionally, about 32% of malfunctions that led to complete postal unit shutdowns during the examined period were hardware-related, of 525 malfunctions out of 1,618 examined. Notably, roughly 80% of all hardware malfunctions lead to end station shutdowns, and about 92% of such malfunctions result in postal unit shutdowns related to computerized equipment, some of which had already been identified for replacement in 2018. This data underscores the detrimental impact of outdated hardware on the operational efficacy of postal units and, consequently, on the quality of service provided to customers.

- **Project for the Replacement of Outdated Computer Equipment at the Postal Company and Postal Bank –** the equipment replacement project[4] was approved within the work plans for 2019–2023. Concurrently, the upgrade to Windows 10 operating systems commenced. This project has been classified as strategic since 2019. However, the Postal Company only began acquiring new computer equipment at the beginning of 2022. As of the audit end date, over four years after the necessity for replacement emerged, numerous malfunctions stem from the delayed equipment replacement, underscoring the urgent need for new equipment. By March 2024, the Company had replaced and upgraded only 683 computers (about 37%) of the required 1,850 computers to Windows 10. By contrast, only 196 (about 56%) of the 350 plasma computers requiring upgrade were upgraded, and only 136 (about 68%) of the 200 queue management systems needing upgrade were completed. The audit also found that annual depreciation on computers and equipment is marginally lower than the purchase values in most years. Total expenditures on computers and peripheral equipment from 2019 to 2022 were NIS 39.8 million, while the total annual depreciation for the same period was NIS 37.4 million (around 94%). These figures indicate that the Company's investments in software and equipment purchases only slightly surpass the depreciation of prior investments. In 2022, investment in software and peripheral equipment purchasing fell below the depreciation of previous years' investments. Hence, the Company maintains the status quo without prioritizing continuous improvement in its information systems.

- **Computerized Queue Management System –** since 2007, the Postal Company and Postal Bank have implemented queue management systems in select postal units using off-the-shelf software. The audit raised that the current system does not facilitate

4 Computers, printers, computerized queue management stations, computer monitors, and other hardware equipment.

customers' input of information regarding the services for which they have reserved a queue[5], nor does it allocate sufficient time based on customer needs. For example, the time required for a customer to open a bank account at the Postal Bank vastly exceeds that allocated for someone collecting a postal package. This discrepancy can lead to excessive wait times at Postal Bank branches, resulting in delayed service. Furthermore, the system cannot log the specific actions customers intend to undertake. Early identification of such actions could inform customers so they are better prepared with the necessary documentation or preparations required for the service. Although customers can independently cancel their queue, the system fails to send reminders to ensure their attendance or cancellation at the designated time. The misalignment between the queue management system and the Company's operational nature and requirements hampers effective queue management, adversely impacting customer service.

- **Multiple Systems and No Interface Among Them –** as of the audit end date, 55 information systems, some of them divided into subsystems, were operational within the Postal Company, with the Postal Bank utilizing an additional 16 systems, some of them are divided into subsystems. These systems are sourced from over 20 different suppliers and employ various technologies. The existence of multiple systems without effective interfaces complicates system integration, diminishes data uniformity, and obstructs process management. This lack of integration creates challenges in synchronizing data across systems, potentially resulting in errors. Consequently, the Company invests in human resources or developing compensatory manual processes to establish system compatibility. For instance, the human resources information system lacks a computerized interface with the Bank's mainframe computer system[6]. When the need arises to revoke an employee's permissions[7] in the mainframe computer system, manual procedures are required: an email is sent from the Human Resources Department to the relevant parties in the mainframe computer system requesting permission revocation. Additionally, a monthly compensatory control process generates an anomaly report for employees who have retired or resigned but remain linked to the mainframe computer system, requiring a manual review of these anomalies. The unique identifiers in the Human Resources Department's information system differ from those in the mainframe computer system. Due to discrepancies in employee registration across both systems, the Company has created a manual conversion table to align employee ID numbers with usernames in the Bank's systems, which must be updated manually to address inconsistencies in data.

- **Periodic Review of Permissions at the Postal Company –** the Postal Company conducts a manual review of permissions for 17 core systems biannually, specifically in January and August. However, permission reviews are not performed for the remaining

5 Other than vehicle ownership transfers.

6 A mainframe computer used to run many applications simultaneously, using large-scale data processing.

7 Due to leaving or retirement.

systems, as mandated by the User and Authorization Procedure. Furthermore, there is no process to document anomalies identified during these reviews, which could assist in pinpointing systems or departments that frequently encounter numerous anomalies, allowing for timely responses. Additionally, no computerized control mechanism is in place to evaluate the alignment of permissions with the permission holders. For instance, when an employee changes positions within the department, the necessary adjustments to their assigned permissions may go unrecognized by the business manager conducting the survey.

- **Review of Permissions in System C at the Postal Company –** the audit found that, as of January 2024, 85 permission holders in System C (constituting 3% of all permission holders in this system) are not classified as "active" in the human resources system. This indicates that the permissions of former employees have not been terminated, or their status was not updated in the human resources system. Despite compensatory automatic controls, errors were detected in the computerized control process, as the audit findings confirmed that 79 employees with active permissions were not identified by the automatic control while also not being marked as "active" in the human resources systems.

- **Permissions in the Central Network Management System at the Postal Company –** the audit found that, as of December 2023, 780 (about 13%) of the active permission holders in the central network management system are employees not recognized as "active" in the Company's human resources system. Among these, 449 (about 58%) have not accessed the central network management system since the onset of 2024. There is a lack of information regarding the last login date for 196 (about 25%) of the permission holders, while it is known that 135 (about 17%) had their last login in 2024. It can be concluded that employees who have not logged in since 2023 and those lacking last login data are likely former employees whose permissions remain active. Moreover, employees who have recently logged-in in 2024, presumably active, still are not listed as "active" in the HR system. Notably, 70 of the 80 employees with active permissions in the audit sample[8] do not work at the Postal Company. Six employees who departed as early as 2020 had yet to have their permissions revoked at the time of sampling, over three years post-departure. The permissions of another employee who left in 2021 and three others who exited in 2023 remain unrevoked. Not revoking permissions for employees who are not "active" could potentially lead to unauthorized access and misuse of valid permissions to the detriment of the Company.

- **Examination of Permissions on the Mainframe Computer at the Postal Bank –** an examination of permissions on the mainframe computer at the Postal Bank raised that 35 users, about 2% of the 1,794 active permissions, belong to employees not classified as active within the human resources systems. While most users must log in to the

8 80 out of 780 active permission holders in the network's central management system are not included in the list of active employees in the Company's human resources system.

central management system before accessing the mainframe computer, these findings pose significant concerns regarding the critical importance of information security at the Bank. Granting active permissions to individuals not employed by the Bank raises the potential risk of compromising information security.

- **Examination of Permissions on the Central Management System of the Postal Bank Network –** a review of the central management system permissions indicated that 67 users with active permissions are either not marked as "active" in the human resources systems or cannot be located. Upon further investigation, it was found that 58 of them are external information systems personnel. An examination of the remaining nine user permissions found that permissions for three employees on maternity leave were not revoked despite the procedural requirement to revoke permissions for employees absent for over one calendar month. One employee, who left the Bank on June 30, 2023, returned to work but remains classified as inactive in the Human Resources Department. Another individual who left the Bank retains permissions, and three active employees are not recognized as such in the human resources systems despite being listed in the alignment table. Moreover, others continue to utilize the username of a former employee. The failure to revoke permissions for individuals deemed inactive within sensitive banking systems compromises the Bank's information security and increases the risk of unauthorized access to its systems.

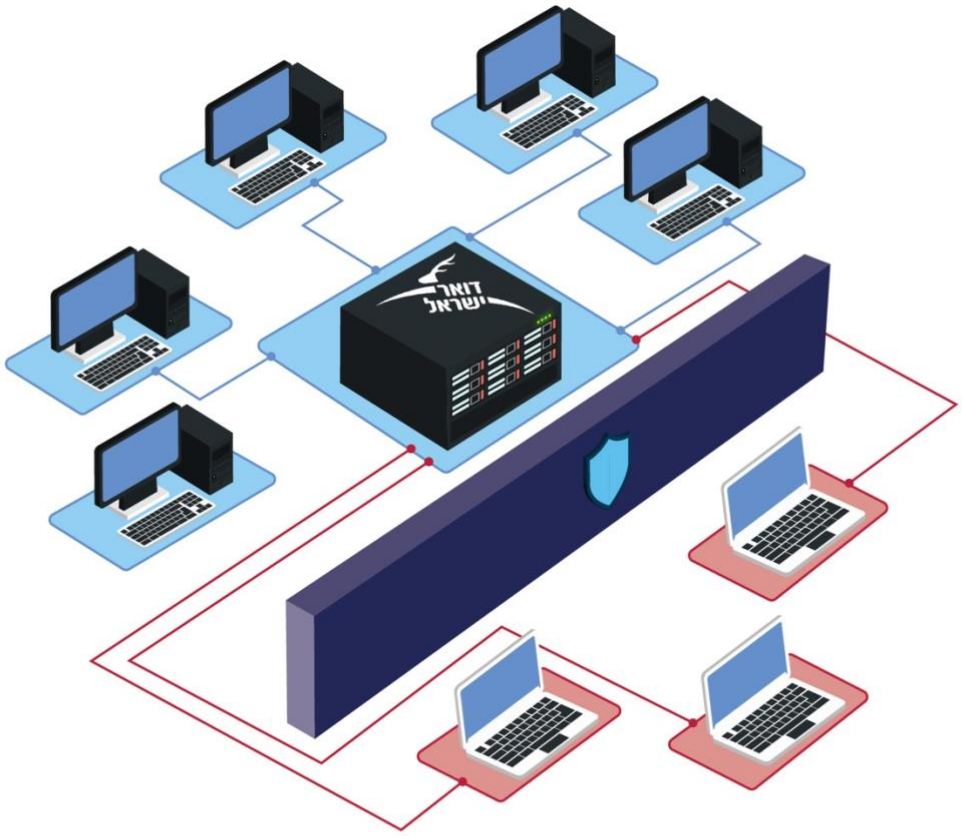
- **Collection Process for Balances from Post Offices –** daily operations involve Company drivers collecting physical references for banking transactions from end stations (balances[9]), placing them in bags, and transferring these to the Postal Bank headquarters at the sorting center in Modi'in. The Company has not met its target of 85% of balances arriving the next day; Currently, only 70% arrive within two days. Control and monitoring of balance arrivals at Postal Bank headquarters are inadequate, with no daily supervision of balances not collected from the preceding business day, preventing confirmation of their arrival at the Postal Company until the monthly audit. Furthermore, no follow-up monitoring is conducted after this inspection. Balances have been left unattended in the sorting hall for extended periods, exposing them to the risk of theft or unauthorized access, which has persisted for years.

9 These balances include, among other things, checks, vouchers, bank forms, and checks for deposit.

Key Recommendations

- The Company should regulate annual and multi-annual work plan issuance and ensure its implementation. This includes evaluating alternatives, monitoring the execution of the work plan, and providing the management of the Information Systems Division with an updated overview of ongoing tasks, their costs, and their scope.
- The Company should promptly complete the project to replace outdated equipment in its units to mitigate risks and enhance customer service.
- The Company should implement the 2021 master plan's recommendations to prevent duplication and unnecessary activities by formulating and developing standardized operational processes that leverage digital and information technologies.
- The Company should conduct routine permission checks within the network's central management system to minimize risks associated with granting access to unauthorized employees and to facilitate permission management across multiple systems. Furthermore, the Company should review the permission-checking process in System C and all other systems under evaluation to identify failures in recognizing inactive employees, particularly concerning the review of manual authorizations. Additionally, it is necessary to locate all employees classified as inactive users who possess permissions in various systems and comprehensively examine the control mechanisms governing user permissions, making improvements based on the findings.
- The Company should enhance control measures at the Postal Bank, regularly reconciling the data of authorized individuals with that from the Human Resources Department. Furthermore, it should develop automated processes for revoking permissions within the Bank's systems and supervise these permissions.

Audit Findings in Examining Permissions in the Central Network Management System at the Postal Company



780

Of the active permission holders in the networks central management system are not included in the list of "active" company employees

Summary

The Postal Company operates 55 information systems, several of which are divided into subsystems, while the Postal Bank utilizes an additional 16 systems, some comprising subsystems. These systems are supported by over 20 suppliers and based on various technologies.

This report raised deficiencies in the information and security systems within the Postal Company and the Postal Bank. Inadequate management of the employee permission revocation process and in controlling this process; Reliance on outdated computer equipment that adversely affects service delivery and jeopardizes information security; Absence of a multi-year strategic plan for the Information Systems Division; Lack of supervision in the execution of work plans; And multiple systems that hinder information transfer, necessitating manual procedures and resource allocation to mitigate these challenges.

The Information Systems Department at the Postal Company should develop a structured action plan that focuses on advancing information systems with a forward-thinking vision, modernization of outdated systems, and optimization of existing systems and their integration, all while ensuring robust cyber protection and minimizing risks associated with unauthorized access.

As part of improving information security, particularly given the recent cyber incident in April 2023, the company should improve control permission management. The Company must address the deficiencies noted in the audit and devise ways to rectify them promptly.