Library and Information Science Research

https://Infosci.um.ac.ir Vol. 16, No 2, 2026

ISSN(Online): 3092-6130 ISSN(Print): 2251-6344 Research Article

The Role of Information Security in Improving Organizational Performance

Adel Soleimani Nezhad
Associate Professor, Department of Knowledge and Information Science, Shahid Bahonar University of Kerman, Kerman, Iran. Email: a.solimani@uk.ac.ir
Fariborz Doroud
Assistant Professor, Iranian Research Institute for Information Science & Technology (IranDoc), Tehran, Iran. (Corresponding Author), Email: doroudi@irandoc.ac.ir
Masoomeh Tahmasbi
M.S.c. in Knowledge and Information Science, Islamic Azad University, Kerman Branch, Kerman, Iran. Email: tahmasbi833@yahoo.com

Abstract

Introduction: In today's knowledge-based economy, organizations increasingly regard knowledge and information as their most valuable strategic assets. However, these assets are highly vulnerable to a wide range of security threats. The rapid expansion of digital technologies and electronic data exchange has significantly increased the exposure of sensitive information to cyberattacks, data breaches, and unauthorized access. Business and public organizations routinely generate, collect, process, and store vast amounts of information, making effective information security management essential for protecting critical organizational assets. Information security management encompasses the policies, procedures, and controls required to safeguard the confidentiality, integrity, and availability of information against potential threats and vulnerabilities. An Information Security Management System (ISMS) provides a systematic framework for managing sensitive organizational information, minimizing security risks, and ensuring business continuity through the proactive mitigation of security incidents. Moreover, an ISMS enables organizations to identify, assess, and address security risks while demonstrating their commitment to information security and privacy. The implementation of an ISMS typically involves information security professionals, including Chief Information Security Officers, IT Operations Managers, Security Coordinators, Security Analysts, and IT administrators, who are responsible for establishing and maintaining appropriate technical and organizational controls. These controls may include security policies, procedures, governance structures, software, and hardware mechanisms designed to protect information assets. Among the internationally recognized frameworks for information security management, **ISO/IEC 27002**, entitled *Information Security, Cybersecurity and Privacy Protection—Information Security Controls*, provides comprehensive guidance on the selection, implementation, and management of information security controls. Accordingly, the present study aims to evaluate the status of information security management practices in government organizations in Kerman, Iran, based

on the human security, monitoring security, and environmental security components of the ISO/IEC 27002 standard. .

Methodology: This study employed a descriptive survey research design. Data were collected using a researcher-developed questionnaire based on the ISO/IEC 27002 standard for information security management. The study population comprised 176 information technology specialists, senior managers, and middle managers employed in government organizations in Kerman, Iran. The sample size was determined using Cochran's formula, resulting in a sample of 120 participants selected from the Departments of Education, the Kerman Governorate, the Tax Affairs Organization, the Agricultural Jihad Organization, and the Department of Industry, Mine and Trade. These organizations were purposively selected to facilitate access to relevant data and information. The questionnaire was developed in accordance with the components of the ISO/IEC 27002 standard, an internationally recognized framework for information security management. It focused on six key domains encompassing 19 subcomponents related to human and environmental security: (1) information security organization (2 subcomponents), (2) human resource security management (3 subcomponents), (3) physical and environmental security management (2 subcomponents), (4) access control (7 subcomponents), (5) information security incident management (2 subcomponents), and (6) compliance management (3 subcomponents). Because the study focused on organizational personnel and security policies, these six domains were incorporated into the research instrument. All items were measured using a five-point Likert scale. The content validity of the questionnaire was confirmed by experts, yielding a content validity coefficient of 0.93. The reliability of the instrument was assessed using Cronbach's alpha, demonstrating satisfactory internal consistency. Data were analyzed using SPSS software. Descriptive statistics were employed to summarize the data, while inferential analyses were conducted after verifying the assumptions of normality using the Kolmogorov–Smirnov test and homogeneity of variances. One-way analysis of variance (ANOVA) was used to test the research hypotheses, and the Friedman test was applied to rank the dimensions of information security management.

Findings: The results of the Kolmogorov–Smirnov test confirmed that all research variables satisfied the assumption of normality. At the 95% confidence level ($\alpha = 0.05$), the null hypothesis of normal distribution was not rejected, justifying the use of parametric statistical tests. Accordingly, one-sample Student's *t*-tests were conducted to examine the main research hypothesis and to compare the mean scores of each dimension of information security management with the expected benchmark. The findings from the six sub-hypotheses indicated that five dimensions—**human resource security management, physical and environmental security, access control, information security incident management, and compliance management**—achieved mean scores that were significantly higher than the expected level ($p < 0.05$). In contrast, the **information security organization** dimension performed below the expected level, indicating a relative weakness in organizational security governance. Overall, the results support the main research hypothesis, demonstrating that the overall performance of

information security management in the government organizations of Kerman, as assessed against the **ISO/IEC 27002** standard, is significantly above the expected level.

Discussion & Conclusion: The findings of the study indicate that information security policy management is not adequately implemented in government organizations in Kerman. Among the organizations examined, the highest level of performance in this dimension was observed in the Governorate, whereas the lowest level was reported in the Agricultural Jihad Organization. These findings suggest that the fundamental theoretical principles underlying information security policy management have not received sufficient attention within these organizations. An effective information security policy should reflect managerial commitment and clearly define the organization's strategic approach to information security management. However, the results indicate that key elements, including the overall objectives, scope, significance, and framework of information security, have not been sufficiently established. Furthermore, information security policies are not systematically reviewed and updated at predetermined intervals, which may reduce their effectiveness in addressing evolving security challenges. Based on the findings, several recommendations are proposed. These include developing a comprehensive information security management plan aligned with environmental, access control, and human resource security requirements; providing specialized and continuous training programs for managerial and technical personnel; strengthening legal frameworks for controlling and monitoring information security activities; maintaining continuous records of security incidents; accurately defining access levels to information resources; ensuring compliance with intellectual property rights in the use of organizational information resources; and facilitating information sharing in accordance with information security management principles.
Keyword: Performance Evaluation; Information Security Management; ISO/IEC 27002; Government Organizations; Kerman City.

پژوهش‌نامه کتابداری و اطلاع رسانی
مقاله پژوهشی https://infosci.um.ac.ir دسترسی آزاد

نقش امنیت اطلاعات در بهبود مؤلفه‌های امنیت انسانی، نظارتی و محیطی

عادل سلیمانی نژاد
دانشیار، گروه علم اطلاعات و دانش‌شناسی، دانشگاه شهید باهنر کرمان، کرمان، ایران. a.solimani@uk.ac.ir
فریبرز درودی
استادیار، پژوهشگاه علوم و فناوری اطلاعات ایران(ایرانداک)، تهران، ایران. (نویسنده مسئول)، doroudi@irandoc.ac.ir
معصومه طهماسبی
کارشناسی ارشد علم اطلاعات و دانش‌شناسی، دانشگاه آزاد اسلامی واحد کرمان، کرمان، ایران. tahmasbi833@yahoo.com

چکیده

مقدمه و هدف: امنیت اطلاعات با اجرای مجموعه‌ای مناسب از نظارت‌ها، شامل سیاست‌ها، قوانین، فرآیندها، رویه‌ها، ساختارهای سازمانی و عملکردهای نرم‌افزاری و سخت‌افزاری حاصل می‌شود. ایزو/ آی‌ای‌سی ۲۷۰۰۲، استاندارد امنیت اطلاعات است که توسط سازمان بین‌المللی استاندارد با عنوان امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی و کنترل‌های امنیت اطلاعات منتشر شده است. هدف این پژوهش، ارزیابی وضعیت فعالیت مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان بر مبنای مؤلفه‌های امنیت انسانی، نظارت و محیطی استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ است.

روش‌ها: روش پژوهش حاضر توصیفی-پیمایشی است و برای جمع‌آوری داده‌ها از پرسشنامهٔ استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲، استفاده شده است. جامعهٔ آماری پژوهش شامل، ۱۷۶ نفر از کارشناسان فناوری اطلاعات و مدیران اصلی و میانی شاغل در سازمان‌های دولتی شهر کرمان است. نمونهٔ جامعه آماری با استفاده از فرمول کوکران، شامل، ۱۲۰ نفر از سازمان‌های آموزش‌وپرورش، استانداری کرمان، امور مالیاتی، جهاد کشاورزی و صنایع و معادن که با هدف دسترسی به آمار و اطلاعات انتخاب شده‌اند، تعیین شد. تحلیل داده‌ها از طریق آمار توصیفی و استنباطی و با استفاده از نرم‌افزار آماری اس‌پی‌اس‌اس صورت گرفته است.

یافته‌ها: با توجه به نتایج به‌دست‌آمده از فرضیهٔ پژوهش، به‌دلیل آنکه p- مقدار به‌دست‌آمده از آزمون کمتر از سطح معنی‌داری تحقیق (۰/۰۵) است می‌توان بیان کرد که میانگین نمرهٔ عملکرد مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان بر مبنای استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ بالاتر از حد انتظار است.

بحث و نتیجه‌گیری: تدوین برنامهٔ مدیریت امنیت اطلاعات براساس مؤلفه‌های مورد بررسی ازنظر مسائل محیطی، دسترسی، و نیروی انسانی؛ برگزاری دوره‌های آموزشی مناسب و تخصصی برای نیروی انسانی سازمان‌ها در سطوح مدیریتی و کارشناسی؛ ملاحظات حقوقی در کنترل و نظارت بر فعالیت مدیریت امنیت اطلاعات؛ ثبت رخدادهای امنیتی به‌صورت مستمر؛ تعیین سطوح

اصالت: نتایج حاصل از این پژوهش براساس استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ نقش مؤثری در برنامه‌ریزی و مدیریت سازمان‌های خدماتی متعدد دارد.

کلیدواژه‌ها: ارزیابی عملکرد، مدیریت امنیت اطلاعات، ایزو آی‌ای‌سی ۲۷۰۰۲، سازمان‌های دولتی، شهر کرمان

مقدمه

امنیت اطلاعات موضوع مهمی است که هرروز بیشتر مورد توجه سازمان‌ها در سراسر جهان قرار می‌گیرد (Elattresh et al., 2019) و آگاهی از مفاهیم آن جزء حیاتی این حوزهٔ کاری در سازمان‌ها است (Hutchinson & Ophoff, 2020). حفاظت از دارایی‌های سازمان‌ها یکی از مهم‌ترین جنبه‌هایی است که سازمان‌ها باید با آن سروکار داشته باشند (Benqdara, 2023) و آگاهی از امنیت اطلاعات مفهوم مهمی است که اخیراً مورد توجه قرار گرفته است (Rohan et al., 2023) و با حفاظت از داده‌ها و اطلاعات در تمام اشکال آن سروکار دارد (Orozova et al., 2019). در عصری که مشخصهٔ آن پیوند رقمی است، نمی‌توان اهمیت امنیت اطلاعات را نادیده گرفت (Weng, 2024) و درک اینکه امنیت سایبری چیست و چگونه می‌توان آن را با موفقیت در فرهنگ امروزی که توسط فناوری و ارتباطات شبکه هدایت می‌شود، به کار برد، حیاتی است (Choppara et al., 2022). لذا، سازمان‌ها ابتدا باید تهدیدات خاصی را که ممکن است با آن مواجه باشند، درک کرده (Lincke, 2024) و متعاقب آن، باید بدانند که امنیت اطلاعات زمانی افزایش می‌یابد که کارکنان حس قوی در باب نظارت دارایی‌های اطلاعاتی داشته باشند (Vedadi et al., 2024).

بیان این نکته ضروری است که تهدیدهای دیجیتالی در حال رشد است (Nowicka et al., 2024) و با توجه به ارزش و تنوع داده‌هایی که سازمان‌ها در فعالیت‌های خود استفاده و تولید می‌کنند، حفاظت از این دارایی بسیار مهم است (Lopes et al., 2022). همچنین، باید توجه کرد که هم‌سو نبودن با مقولهٔ امنیت اطلاعات مسئلهٔ اصلی در سازمان‌ها بوده است (Alam & Xiao, 2022) و انطباق با خط‌مشی امنیت اطلاعات کارکنان نیز فشار قابل توجهی بر اجرای مدیریت آن وارد می‌کند (Liu et al., 2022)؛ ولی، به‌منظور رسیدگی به مسئولیت‌های نظارتی و قانونی خود و حفظ مشارکت‌های راهبردی قابل‌اعتماد، شرکت‌ها باید به تضمین حریم خصوصی، دسترسی و صحت داده‌های در اختیار خود بپردازند (Kitsios et al., 2023). به همین دلیل، سازمان‌ها در بخش نیروی انسانی و منابع سرمایه‌گذاری می‌کنند تا اطمینان حاصل کنند که داده‌های حساس شرکت در دستان کارمندان خود امن است (Kaur et al., 2021). لذا باید بیان کرد که امنیت اطلاعات حوزهٔ

وسیعی است که زمینه‌های مطالعاتی و کاربردی قابل توجهی ازجمله: امنیت فیزیکی، امنیت دسترسی، رمزگذاری داده‌ها و امنیت پایگاه اطلاعاتی و شبکه را پوشش می‌دهد.

سازمان‌ها می‌توانند با رعایت امنیت اطلاعات، به‌عنوان دارایی اطلاعاتی و داده‌محور، به مزیت راهبردی دست یابند (Ma, 2022). همچنین، پژوهش‌های امنیتی موجود در نظام‌های اطلاعاتی، انواع مختلفی از عوامل فردی و سازمانی مؤثر بر رفتارهای امنیت اطلاعات را شناسایی و بررسی کرده‌اند (Lin & Luo, 2021). مشاهده می‌شود که سازمان‌ها در سراسر جهان سرمایه‌گذاری‌های هنگفتی را در اقدامات متقابل فناوری امنیت اطلاعات انجام می‌دهند (Khando et al., 2021). از همین‌رو، مدیریت امنیت اطلاعات مؤثر به ایجاد محیط دیجیتال سازمانی سالم کمک می‌کند (Chen & Hai, 2024). علاوه‌بر آن، بسیاری از یافته‌های پژوهش‌های امنیت اطلاعات به راه‌حل‌هایی محدود می‌شود که بر ابعاد فنی متمرکز هستند (Ejigu et al., 2021). در نتیجه، فرهنگ مطلوب و یا قوی در ارتباط با امنیت اطلاعات می‌تواند تهدید انسانی برای حفاظت از اطلاعات را پایین بیاورد (da Veiga et al., 2020). باید اظهار کرد که در زمینهٔ امنیت اطلاعات، محیط اجتماعی سازمانی نقش مهمی در جلوگیری از تخلفات کارکنان از سیاست امنیت اطلاعات دارد (Yazdanmehr et al., 2024) و حوادث نقض امنیت می‌تواند صرف‌نظر از اینکه با چه کیفیتی از فناوری محافظت می‌شود، در سازمان اتفاق بیفتد (Benqdara, 2023). لذا انجام برنامه‌های حفاظتی و رعایت سیاست‌های امنیت اطلاعات نقش مهمی در بهبود عملکرد سازمان‌ها دارد که باید به‌دقت مورد بررسی قرار گرفته و اجرایی شود.

با عنایت به سنجش وضعیت سازمان‌های مهم دولتی که ازنظر ساختار و فعالیت در تعداد زیادی از شهرهای کشور و مناطق مختلف دارای ویژگی‌های مشابه هستند و نقش مؤثری در فعالیت‌های جامعه دارند، این پژوهش می‌تواند مورد استفاده بسیاری از سازمان‌ها در سطح کشور قرار گیرد. هدف اصلی پژوهش حاضر نیز عبارت است از سنجش وضعیت عملکرد مدیریت امنیت اطلاعاتِ کارکنان در سازمان‌های دولتی شهر کرمان بر مبنای استاندارد بین‌المللی ایزو ۲۷۰۰۲. بر همین اساس پرسش‌های پژوهش نیز در ادامه بیان می‌شود:

عملکرد سازمان‌های دولتی شهر کرمان در زمینهٔ ۱) سیاست مدیریت امنیت اطلاعات؛ ۲) امنیت منابع انسانی سازمان؛ ۳) امنیت فیزیکی و محیطی سازمان؛ ۴) کنترل‌های دسترسی؛ ۵) مدیریت بحران امنیت اطلاعات؛ و ۶) مقایسهٔ سازمان، بر مبنای استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ در چه وضعیتی است؟

فرضیهٔ پژوهش حاضر نیز عبارت است از: میانگین امتیاز فعالیت مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان براساس استاندارد مورد نظر، بیشتر از حد انتظار است.

پیشینه

پژوهش‌های متعددی در بازهٔ استاندارد امنیت اطلاعات و حوزه‌های وابسته انجام شده که تقریباً از سال ۱۹۹۵ این پژوهش‌ها شروع شده است. با عنایت به لزوم مطرح ساختن موضوع‌های جدید و نوآورانه، توجه به حوزه‌های روزآمد ضروری است و ازجمله موضوع‌های مهم می‌توان به این موارد اشاره کرد: افشای اطلاعات محرمانه و حساس (Ibnugraha et al., 2021)؛ تضمین حریم خصوصی و حفاظت از داده‌ها (Farid, Hasan et al., 2021; Shiau et al., 2023 ;Warraich, & Iftikhar, 2023)، امنیت فناوری اطلاعات و شبکه‌ها (Shkarlet et al., 2020;)، مصالحه و حوادث در سازمان‌ها (Antoniou, 2018)، جرایم سایبری[1] (Pietrek & Skelnik, 2023)، رویدادهای مخربی سازمانی (Varsos et al., 2018)، سیاست‌های امنیت (Kinnunen & Siponen, 2018; Kaur et al., 2021; Ifeyinwa Nkemdilim et al., 2022; Alotaibi et al., 2023)، دسترسی غیرقانونی و سوءاستفاده، (Mousavi & Kumar, 2019) و نیز نقش عامل انسانی در امنیت اطلاعات (Petrič Angraini et al., 2021; Lopes et al., 2022; & Orehek, 2024). در ادامه برخی از پژوهش‌های مهم در این عرصه در بخش پژوهش‌های فارسی و انگلیسی بررسی و تحلیل می‌شود.

پژوهش وظیفه و همکاران (Vazife et al., 2019) در رابطه با نظام مدیریت امنیت اطلاعات به انجام رسید. نتایج نشان داد که اطلاع از میزان ارزش اطلاعات، قابلیت بازیابی اطلاعات، استفاده صحیح از منابع و همزیستی اطلاعات و نرم‌افزارها بیشترین ضریب اهمیت را در بین ابعاد ده‌گانه دارد. در نهایت، پس از طی گام‌های پژوهش، الگوی تعیین و استقرار اثربخش نظام مدیریت امنیت اطلاعات در سه لایه شناسایی، ساختار اجرا و طراحی برنامهٔ حمایتی نظام مدیریت امنیت اطلاعات ارائه شد. طهماسبی لیمونی و فلاح‌کردآبادی (Tahmasebi Limooni & Fallah Kordabadi, 2019) در پژوهش خود به بررسی وضعیت به‌کارگیری معماری امنیت اطلاعات در کتابخانه‌های عمومی مازندران پرداختند. نتایج نشان می‌دهد برای برقراری امنیت در هر نظام اطلاعاتی، مدیران و دست‌اندرکاران برقراری امنیت، باید ابعاد و جنبه‌های مختلف امنیتی را مورد توجه قرار دهند، به‌گونه‌ای که در ایجاد نظام اطلاعاتی ایمن به آن‌ها کمک کند. شفیعی نیک‌آبادی و همکاران (Shafiei Nikabadi et al., 2021) به پژوهش دربارهٔ رتبه‌بندی ابعاد مدیریت ریسک امنیت اطلاعات پرداختند. نتایج نشان داد که امنیت ارتباطات رتبهٔ نخست اهمیت را به خود اختصاص می‌دهد. زیرساخت، عوامل انسانی، مدیریت امنیت، کنترل دسترسی به اطلاعات و توسعهٔ نظام‌های اطلاعاتی امن به‌ترتیب در رتبه‌های دوم تا ششم قرار گرفتند. با توجه به نتایج به‌دست‌آمده پیشنهاد شد که سازمان‌ها اقدام به ایجاد گروه مستقل امنیت در سازمان کنند. پژوهش طالبی و تابلی (Talebi & Taboli, 2024) دربارهٔ الگوی ساختاری ـ تفسیری مدیریت

1. cybercrime

امنیت اطلاعات نشان داد که مدل امنیت اطلاعات احتمال دسترسی غیرمجاز به دارایی‌های حساس را به حداقل می‌رساند. اجرای سیاست‌ها و برنامه‌های مدیریت امنیت اطلاعات می‌تواند در جهت بالا بردن اخلاق کاری کارکنان کمک کند و همچنین با افزایش رعایت اخلاق کاری می‌توان مدیریت امنیت اطلاعات را در سازمان افزایش داد. نتایج پژوهش مرزبان و همکاران (Marzban et al., 2025) دربارهٔ مؤلفه‌های انسانی و غیرانسانی در امنیت اطلاعات نشان داد که فرهنگ امنیتی حاصل تعامل پویای سه گروه انسانی است: مدیران ارشد (تصمیم‌گیران راهبردی)، کارکنان (اجراکنندگان رفتارهای روزمره) و تیم‌های فنی (ترجمه‌کنندگان سیاست‌ها به اقدامات عملی).

کارلسون و همکاران (Karlsson et al., 2022) به پژوهش دربارهٔ تأثیر فرهنگ سازمانی بر امنیت اطلاعات کارکنان پرداختند. یافته‌ها نشان داد که فرهنگ‌های سازمانی با تمرکز داخلی به‌طور مثبت با انطباق داده‌های مرتبط با امنیت اطلاعات کارکنان رابطه دارد. همچنین مشخص شد که تفاوت در فرهنگ سازمانی ازنظر کنترل و انعطاف‌پذیری تأثیر کمتری در این مقوله داشته است. کاریا (Kaaria, 2023) به پژوهش دربارهٔ تعیین تأثیر امنیت در نظام اطلاعاتی و منابع انسانی بر عملکرد سازمانی شرکت‌های دولتی تجاری در کنیا پرداخت. در این پژوهش وی به ارائهٔ شاخص‌های مهم در رعایت امنیت اطلاعات در شرکت‌های مبادرت ورزید و نتایج بررسی همبستگی و رگرسیون نشان داد که امنیت اطلاعات با عملکرد سازمانی شرکت‌های تجاری دولتی کنیا رابطهٔ مثبت و معناداری دارد. واگنر (Wagner, 2023) به پژوهش دربارهٔ تأثیر فنون خنثی‌سازی آسیب‌های امنیت اطلاعات سازمانی پرداخت. نتایج پژوهش او نشان داد که عدم‌انطباق فعالیت و عملکرد کارمندان با داده‌هایی که باید با فرایند امنیت اطلاعات حفاظت شوند، شرکت را در معرض حمله عوامل مخرب قرار می‌دهد. همچنین مشخص شد که تخلفات کارکنان در خصوص رعایت امنیت اطلاعات سازمانی، مسئول تقریباً نیمی از حوادث امنیتی است که سازمان‌ها را در معرض آسیب مالی و اعتباری قرار می‌دهد. أیتوق و همکاران (AITooq et al., 2024) در پژوهش خود به موضوع ارتقای موفقیت سازمانی از طریق اشتراک دانش و حاکمیت امنیت اطلاعات مبادرت ورزیدند. یافته‌ها نشان داد که در چشم‌انداز سازمانی امروز، اشتراک دانش و امنیت اطلاعات به مفاهیم اساسی تبدیل شده است. به‌اشتراک‌گذاری دانش، زمانی که به‌طور یکپارچه با چهارچوب امنیتی قوی ادغام شود، به‌عنوان محرک حیاتی برای موفقیت سازمان ظاهر می‌شود. همچنین مشخص شد که تلاش سازمان‌ها برای بهره‌گیری از دانش موجود به‌منظور ارتقای اهداف خود، سبب یافتن راه‌های جدیدی برای تقویت فعالیت‌های اشتراک دانش و پرورش فرهنگ تبادل دانش میان کارکنان، شرکا و تأمین‌کنندگان می‌شود. آکلو (Akello, 2024) در پژوهشی به تحلیل تهدیدهای امنیت اطلاعات سازمانی مبادرت ورزید. نتایج نشان داد که اهمیت اجرای اقدامات امنیتی قوی، مانند فایروال‌ها، نظام‌های تشخیص

نفوذ، فناوری‌های رمزگذاری، و شیوه‌های کُدگذاری ایمن، برای محافظت در برابر تهدیدهای خارجی نقش مؤثری در حفاظت از اطلاعات سازمانی دارد. یافته‌ها حاکی از آن بود که اهمیت آگاهی کاربر، آموزش و پایبندی به سیاست‌ها و رویه‌های امنیتی، سبب حفاظت از داده‌های باارزش سازمانی است. سیکانوفسکی و همکاران (Ciekanowski et al., 2024) به مقولهٔ شناسایی نقش مدیر امنیت اطلاعات در تأمین امنیت در سازمان پرداختند. یافته‌های پژوهش نشان داد که فرآیند توسعه، پیاده‌سازی، حفظ، بهبود و ممیزی سیستم مدیریت کیفیت بر سطح امنیت سازمان تأثیر می‌گذارد و ساختار و خلاقیت همه کارکنان را در بر می‌گیرد. علاوه‌بر آن، پژوهشگران نقش مدیر ارشد امنیت اطلاعات در سازمان را تحلیل می‌کنند و وظایف، مسئولیت‌ها و انتظاراتی را که بر عهده فردی است که این نقش را انجام می‌دهد توضیح می‌دهند. استانوجویچ و ایزگارویچ (Stanojević & Izgarević, 2025) به پژوهش دربارهٔ نقش مدیریت منابع انسانی در ارتقای فرهنگ امنیت اطلاعات سازمانی پرداختند. نتایج نشان داد که شناسایی، ارزیابی و کاهش آسیب‌پذیری‌های مرتبط با اقدامات انسانی نقش مهمی در ایجاد امنیت سازمانی دارد. این حوزه، شامل مسائلی مانند فریب خوردن در دام کلاهبرداری‌های فیشینگ، تهدیدات داخلی و سوء مدیریت داده‌ها است. یافته‌ها حاکی از آن بود که همسوسازی برنامه‌های آگاهی‌بخشی امنیتی با فرهنگ و ارزش‌های کلی سازمان در ارتباط نزدیکی است. پژوهش نان و همکاران (Nan et al., 2026) دربارهٔ کاربرد داده‌کاوی فازی و امنیت اطلاعات شبکه مبتنی بر شبکه‌های حسگر در مدیریت منابع انسانی سازمانی به انجام رسید. نتایج نشان داد که می‌توان چهارچوب امنیت اطلاعات شبکه را برای نظام اطلاعات مدیریت منابع انسانی کم‌هزینه طراحی کرد و از سازوکارهای حفاظتی چندلایه مانند فناوری رمزگذاری، کنترل دسترسی و سیستم‌های تشخیص نفوذ برای اطمینان از محرمانگی، یکپارچگی و در دسترس بودن داده‌ها استفاده کرد.

بررسی پیشینه پژوهش نشان می‌دهد که مؤلفه‌های متعددی در حوزهٔ امنیت اطلاعات سازمانی تأثیر دارند. فرهنگ سازمانی، توانایی کارکنان و نیروی انسانی، معماری امنیت اطلاعات، ساختار امنیتی نظام‌های اطلاعاتی و فناوری، هنجارهای سازمانی و ارتقاء نظام اداری، همگی در این زمینه مؤثر هستند. همچنین، نقش مدیر امنیت اطلاعات با توجه به استانداردهای موجود و مقابله با تهدیدهای پیش‌رو، براساس بهبود و ممیزی سیستم مدیریت کیفیت؛ چالش‌های مرتبط با امنیت اطلاعات سازمانی، ساختارهای امنیتی و شاخص‌های بررسی فعالیت‌های مرتبط با امنیت اطلاعات، اجرای اقدامات امنیتی قوی، نظام‌های تشخیص نفوذ، فناوری‌های رمزگذاری، و شیوه‌های کُدگذاری ایمن ازجمله مقوله‌هایی است که در پژوهش‌ها مورد توجه قرار گرفته است و با عنایت به آنکه نقش استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ در این پژوهش‌ها چندان مورد نظر قرار نگرفته، و

این استاندارد شرایط مطلوبی برای بررسی و تحلیل شاخص‌ها و مؤلفه‌های امنیت اطلاعات دارد، پژوهش پیش‌رو به‌منظور رفع این خلأ پژوهشی انجام شده است.

روش‌ها

پژوهش حاضر از روش پیمایشی ـ توصیفی بهره می‌گیرد. در این پژوهش، جامعهٔ آماری شامل تمامی مدیران اصلی و میانی سازمان‌های دولتی شهر کرمان و نیز متخصصان فناوری اطلاعات هستند. از میان ۸۹ سازمان دولتی، تعداد ۵ سازمان از طریق نمونه‌گیری هدفمند انتخاب شدند. این سازمان‌ها عبارت‌اند از: استانداری کرمان، جهاد کشاورزی، ادارهٔ کل آموزش‌وپرورش، امور مالیاتی، و سازمان صنایع و معادن استان. در میان این جامعهٔ آماری، تعداد ۱۷۶ نفر که دارای پُست‌های مورد نظر (مدیران و کارکنان) بودند، شناسایی شدند. با استفاده از فرمول کوکران نمونه‌گیری این جامعهٔ آماری، ۱۲۰ نفر تعیین شد.

بر این اساس، در جدول (۱)، حجم نمونهٔ مورد بررسی به تفکیک سازمان، تعداد کل و نمونه انجام‌شده بیان شده است.

جدول ۱. تعداد مدیران عالی، مدیران میانی و کارشناسان فناوری اطلاعات سازمان‌های دولتی شهر کرمان به تفکیک سازمان و تعداد نمونه

سازمان	تعداد کل	تعداد نمونه
آموزش‌وپرورش	۳۸	۲۶
استانداری کرمان	۶۸	۴۶
امور مالیاتی	۳۳	۲۳
جهاد کشاورزی	۲۱	۱۴
صنایع و معادن	۱۶	۱۱
جمع کل	۱۷۶	۱۲۰

به‌منظور جمع‌آوری داده‌های پژوهش از پرسشنامه محقق‌ساخته استفاده شد. پرسشنامه بر مبنای مؤلفه‌های استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ طراحی شد. این منبع، استاندارد کاربردی و مورد تأیید سازمان بین‌المللی استانداردسازی در زمینهٔ امنیت اطلاعات است که در اواسط ۱۹۹۰ منتشر شده است. این استاندارد با عنوان ISO/IEC 17799:2000 با ISO/IEC سازگار شد، در سال ۲۰۰۵ بازبینی شد، و در سال ۲۰۰۷ با

تغییر شماره (اما در غیر حال بدون تغییر) با مجموعه استانداردهای ۲۷۰۰۰ تطبیق داده شد. اهمیت آن در پوشش مناسب تمامی شاخص‌ها و مؤلفه‌های امنیت اطلاعات است. لذا در این پژوهش از آن بهره گرفته شد.

با عنایت به حیطهٔ پژوهش حاضر، یعنی بررسی مؤلفه‌های مربوط به کارکنان و سیاست‌ها، تعداد ۶ مؤلفهٔ این حوزه انتخاب و در پرسش‌های پژوهش مطرح شد. روایی ابزار پژوهش به روش محتوایی مورد بررسی قرار گرفت که میزان آن ۰/۹۳ تعیین شد. همچنین، برای بررسی همسانی درونی سنجش پایایی پژوهش از روش آلفای کرونباخ بهره گرفته شد.

جدول ۲. سنجش پایایی پرسشنامه براساس آلفای کرونباخ

پرسشنامه	آلفای کرونباخ	تعداد سؤالات	تعداد آزمودنی‌ها
مدیریت امنیت اطلاعات	۰/۹۸	۳۹	۱۲۰

برای تحلیل داده‌های پژوهش به‌منظور بررسی اطلاعات مربوط به پرسش‌ها و فرضیهٔ پژوهش، پس از انجام آزمون کلموگروف ـ اسمیرنوف و تأیید نرمال بودن توزیع داده‌ها با فرض برابری واریانس‌ها در گروه‌های مورد بررسی از تحلیل واریانس[1] و برای رتبه‌بندی از آزمون فریدمن برای بررسی فرضیهٔ پژوهش استفاده شده است.

یافته‌ها

در بررسی ۶ پرسش پژوهش یعنی: فعالیت سازمان‌های دولتی شهر کرمان در زمینهٔ ۱) سیاست مدیریت امنیت اطلاعات؛ ۲) امنیت منابع انسانی سازمان؛ ۳) امنیت فیزیکی و محیطی سازمان؛ ۴) کنترل‌های دسترسی؛ ۵) مدیریت بحران امنیت اطلاعات؛ و ۶) مقایسهٔ سازمان، بر مبنای استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ در چه وضعیتی است؟ یافته‌های حاصل از تحلیل اطلاعات در جدول (۳) ارائه شده است.

جدول ۳. آماره‌های توصیفی شاخص مدیریت سیاست‌های امنیتی در سازمان‌های دولتی کرمان

مؤلفه‌ها	میانگین	انحراف معیار	چولگی	کشیدگی	کمینه	بیشینه	تعداد
سیاست‌های امنیتی	۳/۳۰	۰/۹۴۰	۰/۱۰	-۰/۹۲	۲/۰۰	۵	۱۲۰

1. ANOVA

امنیت منابع انسانی	۴/۲۰	۰/۹۰۱	-۰/۹۹	-۰/۱۶	۲/۰۰	۵	۱۲۰
امنیت فیزیکی و محیطی	۴/۰۲	۰/۹۱۱	-۰/۷۱	-۰/۵۵	۲/۰۰	۵	۱۲۰
کنترل‌های دسترسی	۳/۸۸	۰/۷۷۴	-۰/۳۶	-۰/۸۰	۲/۲۰	۵	۱۲۰
مدیریت بحران	۴/۳۰	۰/۸۳۲	-۰/۸۰	-۰/۳۰	۲/۱۷	۵	۱۲۰
مقایسه سازمانی	۴/۱۸	۰/۸۲۶	-۰/۹۵	۰/۲۴	۲/۰۰	۵	۱۲۰

بر مبنای داده‌های جدول (۳)، و بررسی پرسش اول پژوهش، با توجه به نمرهٔ شاخص مدیریت سیاست‌های امنیتی، و در نظر گرفتن میانگین نمرهٔ محاسبه‌شده (۳/۰۰)، مدیریت سیاست‌های امنیتی در سازمان‌های دولتی شهر کرمان به میزان متوسط بوده است. با توجه به میانگین مدیریت سیاست‌های امنیتی هر سازمان و مقایسهٔ آن با حد انتظار، دربارهٔ این متغیر می‌توان نتیجه گرفت که در سه سازمان آموزش‌وپرورش، استانداری و امور مالیاتی سطح مدیریت سیاست‌های امنیتی بالاتر از حد انتظار است ولی در سازمان جهاد کشاورزی سطح مدیریت سیاست‌های امنیتی کمتر از حد انتظار و در صنایع و معادن سطح مدیریت سیاست‌های امنیتی برابر سطح انتظار است. در بررسی پرسش دوم پژوهش، با توجه به میانگین نمرهٔ محاسبه‌شده (۴/۲۰)، امنیت منابع انسانی سازمان در سازمان‌های دولتی شهر کرمان به میزان زیاد بوده است. با توجه به میانگین امنیت منابع انسانی هر سازمان و مقایسهٔ آن با حد انتظار، دربارهٔ این متغیر، می‌توان نتیجه گرفت که در تمامی این پنج سازمان امنیت منابع انسانی سازمان بالاتر از حد انتظار است. همچنین نتایج مرتبط با پرسش سوم پژوهش نشان داد که با توجه به میانگین نمره محاسبه‌شده (۴/۰۲)، در سازمان‌های دولتی شهر کرمان به میزان زیاد بوده است. با توجه به میانگین این شاخص و مقایسهٔ آن با حد انتظار، دربارهٔ این متغیر می‌توان نتیجه گرفت که در تمامی این پنج سازمان امنیت فیزیکی و محیطی سازمانی بالاتر از حد انتظار است. همچنین بررسی پرسش چهارم پژوهش حاکی از آن است که نمرهٔ شاخص کنترل‌های دسترسی، با توجه به میانگین نمرهٔ محاسبه‌شده (۳/۸۸)، در سازمان‌های دولتی شهر کرمان به میزان زیاد ارزیابی شده است. با عنایت به میانگین آن و مقایسهٔ آن با حد انتظار، دربارهٔ این متغیر، می‌توان نتیجه گرفت که در تمامی این پنج سازمان کنترل‌های دسترسی بالاتر از حد انتظار است. نتایج حاصل از جدول (۳) دربارهٔ پرسش پنجم پژوهش نیز نشان‌دهندهٔ آن است که میانگین نمرهٔ محاسبه‌شده (۴/۳۰)، به میزان زیاد بوده است. با توجه به نمرهٔ میانگین مدیریت بحران هر سازمان و مقایسهٔ آن با حد انتظار، در مورد این متغیر، می‌توان نتیجه گرفت که در تمامی این پنج سازمان مدیریت بحران بالاتر از حد انتظار است. در نهایت بررسی پرسش ششم پژوهش نیز با توجه به میانگین نمرهٔمحاسبه‌شده (۴/۱۸)، مولفهٔ مقایسهٔ سازمان به میزان زیاد بوده است. با توجه به

میانگین مولفهٔ مقایسهٔ سازمان و مقایسهٔ آن با حد انتظار، دربارهٔ این متغیر می‌توان نتیجه گرفت که در تمامی این پنج سازمان مقایسهٔ سازمان بالاتر از حد انتظار است.

در زمینهٔ فرضیه پژوهش، پیش از بررسی باید نرمال بودن توزیع متغیرهای تحقیق توسط آزمون کولموگروف ـ اسمیرنوف یک نمونه‌ای بررسی شود. بر این اساس گزاره‌های زیر مورد بررسی قرار گرفت و نتایج بررسی نشان داد:

H_0 : متغیر مورد بررسی توزیع نرمال دارد.

H_1 : متغیر مورد بررسی توزیع نرمال ندارد.

جدول ۴. آزمون کولموگروف ـ اسمیرنوف برای شاخص‌های سیاست‌گذاری امنیت اطلاعات

مؤلفه‌ها / آزمون آماری	مدیریت سیاست امنیتی	امنیت منابع انسانی	امنیت فیزیکی و محیطی	کنترل و دسترسی	مدیریت بحران	مقایسه سیاست‌گذاری
کولموگروف ـ اسمیرنوف	۱/۲۴۶	۱/۰۶۳	۱/۱۷۸	۱/۶۰۲	۱/۹۳	۱/۷۸
معنی‌داری	۰/۳۰۰	۰/۳۲۱	۰/۲۰۰	۰/۱۱۱	۰/۰۷	۰/۱۳
نتیجه‌گیری	نرمال	نرمال	نرمال	نرمال	نرمال	نرمال

بر مبنای نتایج جدول (۴)، آزمون کولموگروف ـ اسمیرنوف و معنی‌داری به‌دست‌آمده، به‌علت اینکه معنی‌داری به‌دست‌آمده بیشتر از ۰/۰۵ (سطح معنی‌داری پژوهش) است لذا فرض نرمال بودن برای متغیرهای تحقیق مورد تأیید قرار می‌گیرد. یعنی با ۰/۹۵ درصد اطمینان (در سطح معنی‌داری ۰/۰۵) فرض نرمال بودن توزیع متغیرها پذیرفته می‌شود.

به‌دلیل اینکه فرض نرمال بودن برای متغیرهای پژوهش پذیرفته شد برای بررسی فرضیهٔ تحقیق از آزمون پارامتریک تی استفاده شد.

فرضیهٔ پژوهش: میانگین امتیاز مؤلفه‌های فعالیت مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان براساس استاندارد مورد نظر، بیشتر از حد انتظار است.

H_0 : فرضیهٔ پژوهش: میانگین امتیاز مؤلفه‌های فعالیت مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان براساس استاندارد مورد نظر، بیشتر از حد انتظار نیست.

H_1 : فرضیهٔ پژوهش: میانگین امتیاز مؤلفه‌های فعالیت مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان براساس استاندارد مورد نظر، بیشتر از حد انتظار است.

با استفاده از روش t مستقل (استودنت) و میانگین واریانس و نیز با توجه به اینکه در پنج مورد محاسبات سطح معناداری از ($p < ۰/۰۵$) کوچک‌تر به دست آمد، می‌توان به این نتیجه رسید که فعالیت‌های امنیت منابع انسانی، امنیت فیزیکی و محیطی، کنترل و دسترسی، مدیریت بحران و مقایسهٔ سیاست‌گذاری در سازمان‌های دولتی شهر کرمان بیش‌ازحد انتظار و فعالیت مدیریت سیاست امنیتی در این سازمان‌ها پایین‌تر از حد انتظار است.

جدول ۵. تحلیل مؤلفه‌های مدیریت امنیت اطلاعات

مؤلفه‌ها	نسبت واریانس	Sig (p-value)	آزمون تی	درجه آزادی	Sig.(2-taild)	خطای استاندارد
مدیریت سیاست امنیتی	۱/۵۶۷	۰/۰۶	۱/۰۰	۱۲۰	۰/۴۵۶	۰/۱۴۱
امنیت منابع انسانی	۱/۰۸۷	۰/۰۲	۱/۸۷	۱۲۰	۰/۳۱۶	۰/۱۴۰
امنیت فیزیکی و محیطی	۱/۳۲۴	۰/۰۱۸	۱/۰۷۶	۱۲۰	۰/۴۷۳	۰/۱۴۵
کنترل و دسترسی	۱/۷۶۰	۰/۰۳۱	۱/۲۸	۱۲۰	۰/۷۸۴	۰/۱۴۸
مدیریت بحران	۱/۴۵۳	۰/۰۱۲	۱/۳۴	۱۲۰	۰/۴۵۳	۰/۱۲۹
مقایسه سیاست‌گذاری	۱/۲۶۷	۰/۰۳۱	۱/۵۶	۱۲۰	۰/۸۷۵	۰/۱۴۵

با مقایسهٔ موارد محاسبه‌شده در جدول (۵) و با توجه به آماره‌های آزمون T و درجهٔ آزادی ۱۲۰ و همچنین بیشترین نسبت واریانس به‌دست‌آمده برای هر شش فرضیهٔ فرعی پژوهش در خصوص حد انتظار در فعالیت مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان براساس استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ بررسی شد. نتایج حاکی از آن است که هر چه مقدار این نسبت از یک بزرگتر باشد براساس این مقادیر به این نتیجه می‌رسیم که سازگاری داده‌ها و پس از آن عامل اعتبار داده‌ها به‌ترتیب بیشترین تأثیر را در فعالیت مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان داشته‌اند. در نتیجه فعالیت امنیت منابع انسانی

بیشترین تأثیرگذاری و فعالیت مدیریت سیاست‌های امنیتی کمترین تأثیرگذاری و سایر فعالیت‌ها، تأثیرگذاری قابل قبولی را بر مدیریت امنیت اطلاعات داشته‌اند.

جدول ۶. نتایج آزمون تی، مقایسه میانگین‌ها

مؤلفه‌ها	آزمون T مقایسه میانگین‌ها						
متغیر	T	درجهٔ آزادی	P-مقدار	اختلاف میانگین	انحراف معیار	فاصلهٔ اطمینان ۹۵ درصد	
						کران پایین	کران بالا
مدیریت امنیت اطلاعات	۱۶/۳۵۶	۱۱۹	۰/۰۰۰	۱/۰۶۵	۰/۷۰۷	۰/۰۶۴	۰/۹۲۸

*در سطح ۰/۰۵ معنی‌دار (p<۰/۰۵)

با توجه به نتایج به‌دست‌آمده از جدول (۶)، به‌علت اینکه p- مقدار به‌دست‌آمده از آزمون کمتر از سطح معنی‌داری تحقیق (۰/۰۵) است در نتیجه می‌توان گفت که فرض صفر رد می‌شود یا به عبارتی فرض یک مبنی بر اینکه میانگین نمرهٔ عملکرد مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان بر مبنای استاندارد ایزو/ آی‌ای‌سی ۲۷۰۰۲ بالاتر از حد انتظار است مورد قبول واقع می‌شود، لازم به ذکر است که در این پژوهش حد انتظار برابر سطح متوسط بوده است.

بحث و نتیجه‌گیری

بر مبنای یافته‌های پژوهش، مدیریت سیاست‌های امنیتی در سازمان‌های دولتی شهر کرمان به‌خوبی رعایت نمی‌شود. بیشترین سطح مدیریت سیاست‌های امنیتی در استانداری و کمترین آن نسبت به سایر سازمان‌های مورد بررسی در جهاد کشاورزی است. نتایج حاکی از آن است که امنیت اطلاعات، اهداف کلی و دامنهٔ کاربرد و اهمیت آن طبق چهارچوب کلی در این سازمان‌ها به‌خوبی تعریف نشده است و خط‌مشی امنیت اطلاعات در بازه‌های زمانی برنامه‌ریزی‌شده بازبینی نمی‌شود. در خصوص اهمیت و نقش سیاست امنیت اطلاعات و لزوم توجه به آن، نتیجه به‌دست‌آمده با یافته‌های پژوهش کاریا (Kaaria, 2023) و آکلو (Akello, 2024) و طهماسبی لیمونی و فلاح‌کردآبادی (Tahmasebi Limooni & Fallah Kordabadi, 2019) از منظر توجه به سیاست‌گذاری، رتبه‌بندی و لزوم رعایت آن، دارای هم‌سویی است.

چگونگی عملکرد سازمان‌های دولتی در زمینهٔ امنیت منابع انسانی نشان می‌دهد که در تمامی این پنج سازمان امنیت منابع انسانی سازمان بالاتر از حد انتظار است. امنیت نیروی انسانی نقش مهمی در اجرای امنیت اطلاعات دارد؛ این مقوله با پژوهش طالبی و تابلی (Talebi & Taboli, 2024) و نیز مرزبان و همکاران (Marzban et al., 2025) دارای هم‌سویی است. ولی با پژوهش وظیفه و همکاران (Vazife et al., 2019) از جنبهٔ جایگاه اهمیت نقش نیروی انسانی در رعایت امنیت اطلاعات، هم‌سویی کامل ندارد. برای بهره‌گیری از منابع اطلاعاتی سازمان، رعایت امنیت در ابعاد مختلف ازجمله: اشتراک‌گذاری، تسهیم و تعامل با دیگر سازمان‌ها، انتشار و آگاهی‌رسانی به‌منظور ارائهٔ گزارش عملکرد و مانند آن، سبب تقویت بنیهٔ امنیتی می‌شود. پژوهش استانوجویچ و ایزگارویچ (Stanojević & Izgarević, 2025) از این جنبه با یافته‌های پژوهش حاضر دارای اشتراک است. از این منظر، وضعیت امنیت نیروی انسانی برای فعالیت‌های آتی سازمانی مطلوب است. این نتیجه با یافته‌های پژوهش کاریا (Kaaria, 2023) و أیتوق و همکاران (AITooq et al., 2024) از جنبهٔ اهمیت جایگاه نیروی انسانی و لزوم توجه به آن در امنیت سازمانی، به‌ویژه بهره‌گیری از منابع اطلاعاتی سازمانی، دارای اشتراک است. ولی از منظر بروز بیشتر تهدیدات از جایگاه خطاهای کارکنان با پژوهش واگنر (Wagner, 2023) دارای هم‌سویی نیست.

شرایط مطلوب شاخص امنیت فیزیکی و محیطی سازمان، حاکی از آن است که حفاظت امنیتی محیطی ازنظر فیزیکی و ازجمله، ورودها و خروجی‌ها، حفاظ‌های امنیتی، بررسی پذیرش افراد و مراجعان براساس شاخص‌های کنترلی نظیر، استفاده از کارت‌های هوشمند و چهره‌نگار در شرایط خوبی قرار گرفته است. علاوه‌بر آن، نظارت بر امکانات پشتیبانی ازجمله زیرساخت‌های برق، شبکه، خطوط اینترنت، کابل‌ها و سیم‌ها، بهره‌گیری از رایزرهای ایمن و مانند آن در این میان نقش مهمی برعهده دارد. این امر سبب می‌شود تا نظارت بهتری ازنظر محیطی در سازمان ایجاد شود و امکان پردازش و تحلیل اطلاعات مرتبط مهیا باشد. کنترل‌های ورودی برای گزارش‌های امنیتی نقش مهمی برعهده دارد؛ زیرا تهدیدهای بیرونی را کاهش می‌دهد و سبب جلوگیری از حوادث ناخواسته می‌شود. این یافته با نتایج پژوهش نان و همکاران (Nan et al., 2026) سیکانوفسکی و همکاران (Ciekanowski et al., 2024) ازنظر تهدیدهای محیطی دارای هم‌سویی است؛ ولی از جنبهٔ تناسب نقش فناوری و نیروی انسانی با پژوهش آکلو (Akello, 2024) دارای اشتراک کامل نیست.

نتایج نشان می‌دهد که شاخص کنترل‌های دسترسی به میزان زیاد بوده است و می‌توان نتیجه گرفت که در تمامی این پنج سازمان کنترل‌های دسترسی بالاتر از حد انتظار است. باید توجه کرد که کنترل دسترسی یکی از شاخص‌هایی است که باید همواره در دستور کار قرار گیرد و به‌صورت مداوم اجرایی شود. معمولاً دسترسی‌های کاربران براساس نیاز سازمان در انجام فعالیت‌های حرفه‌ای و نوع کار تعریف می‌شود.

رعایت ایمنی در کاربرد حساب کاربری و رمز عبور، سطوح دسترسی، سنجش هویت کاربران، حفاظت از اطلاعات حساس و نیز کنترل‌های عمیق در ورود و استفاده از نظام‌ها و شبکه‌های سازمانی از زمرهٔ مسائل مهم در رعایت امنیت اطلاعات است. این یافته با نتایج پژوهش کارلسون و همکاران (Karlsson et al., 2022) و نیز کاریا (Kaaria, 2023) دارای هم‌سویی است.

مدیریت بحران در سازمان‌های دولتی شهر کرمان به میزان زیاد بوده است و می‌توان نتیجه گرفت که در تمامی این پنج سازمان مدیریت بحران بالاتر از حد انتظار است. در این رابطه، باید بیان کرد که بررسی وقایع امنیتی یکی از عوامل مهم در سنجش این زمینه است. باید تلاش شود تا در زمان کوتاه، مدیریت امنیت اطلاعات بتواند گزارش‌های مناسب را تدوین کرده و براساس آن اقدام مناسب انجام دهند. تحلیل شواهد موجود دربارهٔ اقدام‌های انجام‌گرفته حقوقی و قضایی می‌تواند نقش مؤثری در راستای حفاظت امنیتی داشته باشد. در مجموع می‌توان نتیجه گرفت که تطابق در سازمان‌های دولتی شهر کرمان به میزان زیاد بوده است. بر این اساس، در تمامی این پنج سازمان تطابق سازمانی در حوزهٔ مدیریت امنیت اطلاعات بالاتر از حد انتظار ارزیابی می‌شود. براساس نتایج به‌دست‌آمده پیشنهاد می‌شود:

برنامهٔ تدوین مدیریت امنیت اطلاعات براساس مؤلفه‌های مورد بررسی ازنظر مسائل محیطی، دسترسی، و نیروی انسانی در این سازمان‌ها تدوین شود.

دوره‌های آموزشی مناسب و تخصصی برای نیروی انسانی سازمان‌ها در سطوح مدیریتی و کارشناسی برگزار شود.

ملاحظات حقوقی از منظر کنترل و نظارت بر فعالیت مدیریت امنیت اطلاعات توسط سازمان‌ها لحاظ شود.

رخدادهای امنیتی و وقایع مرتبط، به‌صورت مستمر ثبت و گزارش شود. سپس براساس این اسناد، خط‌مشی مدیریت امنیتی روزآمد و اصلاح شود.

سطوح دسترسی به منابع اطلاعاتی به‌صورت دقیق و مدون مشخص و رعایت شود.

حقوق مالکیت فکری و حق مؤلف سازمان‌ها در زمینه بهره‌گیری از منابع اطلاعاتی به رسمیت شناخته شده و رعایت شود.

اشتراک‌گذاری اطلاعات با رعایت الزامات مدیریت امنیت اطلاعات به‌صورت کامل رعایت شود.

پایگاه‌های اطلاعاتی و نظام‌های اطلاعاتی از استانداردهای امنیتی به‌صورت کامل پیروی کنند.

References

AITooq, R., Barnawi, N., & Alhamed, A. (2024). Enhancing Organizational Success through Knowledge Sharing and Information Security Governance: A Comprehensive Survey. *Proceedings of the 10 th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'24), Barcelona, Spain - August 19 - 21*. doi:10.11159/cist24.163

Akello, B. O. (2024). Organizational information security threats: Status and challenges. *World Journal of Advanced Engineering Technology and Sciences*, *11*(1), 148–162.

Alam, M., & Xiao, N. (2022). How Does Organizational Justice Work Across National Culture? Effects of Procedural and Distributive Justice on Information Security Policy Compliance Across National Culture.

Alotaibi, F. M., Al-Dhaqm, A., Yafooz, W. M., & Al-Otaibi, Y. D. (2023). A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field. *Applied Sciences*, *13*(17), 9703.

Angraini, Alias, R. A., & Okfalisa. (2021). *Information Security Policy Compliance: An Exploration of User Behaviour and Organizational Factors.* Paper presented at the International Conference of Reliable Information and Communication Technology.

Antoniou, G. S. (2018). *A Framework for the Governance of Information Security: Can it be Used in an Organization.* Paper presented at the SoutheastCon 2018.

Benqdara, S. (2023). Building an Information Security Awareness Program for a Private Financial Organization: Case from Libya. *International Journal of Computer Applications*, *975*, 8887.

Chen, H., & Hai, Y. (2024). Exploring the critical success factors of information security management: a mixed-method approach. *Information & Computer Security*.

Choppara, M., Varanasi, A., Minocha, J., & Sameera, K. H. (2022). Digitalised Information Security in Data Communication in Organizational Flow. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *10*(6), 2825–2829.

Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., & Czech, A. (2024). Chief information security officer: a vital component of organizational information security management.

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. doi:https://doi.org/10.1016/j.cose.2020.101713

Ejigu, K., Siponen, M., & Muluneh, T. (2021). *Influence of Organizational Culture on Employees Information Security Policy Compliance in Ethiopian Companies.* Paper presented at the Pacific Asia Conference on Information Systems.

Elattresh, U. J., Ramadan, K., & Tokeser, U. (2019). Factors Effecting Information Security Management and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC). *Australian Journal of Basic and Applied Sciences*, *13*(10), 99–107.

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science, 0*(0), 01655515231160026. doi:10.1177/01655515231160026

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58*, 102726. doi:https://doi.org/10.1016/j.jisa.2020.102726

Hutchinson, G., & Ophoff, J. (2020, 2020//). *A Descriptive Review and Classification of Organizational Information Security Awareness Research.* Paper presented at the Information and Cyber Security, Cham.

Ibnugraha, P. D., Nugroho, L. E., & Santosa, P. I. (2021). Risk model development for information security in organization environment based on business perspectives. *International Journal of Information Security, 20*(1), 113–126. doi:10.1007/s10207-020-00495-7

Ifeyinwa Nkemdilim, O., Aguboshim, F. C., & Nwajikwa, C. S. (2022). MANAGING ORGANISATION INFORMATION SECURITY SYSTEMS, CONFLICTS, AND INTEGRITY FOR SUSTAINABLE AFRICA TRANSFORMATION. *ANSPOLY JOURNAL OF INNOVATIVE DEVELOPMENT (AJID), 1*(2), 30–39.

Kaaria, A. G. (2023). Human Resource Information Systems Information Security and Organizational Performance of Commercial State Corporations in Kenya. *East African Journal of Information Technology*, *6*(1), 256–278.

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security, 30*(3), 382–401.

Kaur, J., Dhillon, G., & Picoto, W. N. (2021). The role of organizational competence on information security job performance.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267. doi:https://doi.org/10.1016/j.cose.2021.102267

Kinnunen, H., & Siponen, M. (2018). *Developing organization-specific information security policies by using critical thinking.* Paper presented at the Pacific Asia Conference on Information Systems.

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. *Sustainability, 15*(7), 5828.

Lin, C., & Luo, X. (2021). Toward a unified view of dynamic information security behaviors: insights from organizational culture and sensemaking. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52*(1), 65–90.

Lincke, S. (2024). *Information Security Planning: A Practical Approach*: Springer Nature.

Liu, C., Liang, H., Wang, N., & Xue, Y. (2022). Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender. *Information Technology & People, 35*(2), 802–834. doi:10.1108/ITP-09-2019-0452

Lopes, A., Reis, L., São Mamede, H., & Santos, A. (2022, 2022//). *Information Security Threat Assessment Using Social Engineering in the Organizational Context – Literature Review*. Paper presented at the Information Systems and Technologies, Cham.

Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management, 59*(1), 102744. doi:https://doi.org/10.1016/j.ipm.2021.102744

Marzban, m. h., Sharifzadeh, r., & Poorebrahimi, A. (2025). Identifying the Human-Nonhuman Components of Information Security Culture: A Qualitative Study Based on Actor-Network Theory (ANT). *Human Information Interaction*, *12*(2), 46–70. Retrieved from http://hii.khu.ac.ir/article-1-3225-fa.html. [In Persian]

Mousavi, M. Z., & Kumar, S. (2019). *Analysis of key factors for organization information security*. Paper presented at the 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon).

Nan, H., Chen, D., & Bing, Z. (2026). Application of fuzzy data mining and network information security based on sensor networks in enterprise human resource management. *International Journal of System Assurance Engineering and Management*, 1–9.

Nowicka, J., Ciekanowski, Z., & Milewska, A. (2024). Information Security Management as the Basis for the Functioning of an Organization.

Orozova, D., Kaloyanova, K., & Todorova, M. (2019). Introducing information security concepts and standards in higher education. *TEM Journal, 8*(3), 1017.

Petrič, G., & Orehek, Š. (2024). Expressing opinions about information security in an organization: the spiral of silence theory perspective. *Information & Computer Security, ahead-of-print*(ahead-of-print). doi:10.1108/ICS-04-2024-0083

Pietrek, G. W., & Skelnik, K. (2023). CYBERSECURITY AND THE SCOPE OF DESIGNING INFORMATION SECURITY SYSTEMS IN THE ORGANIZATION. *Journal of Modern Science, 51*(2).

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon, 9*(3). doi:10.1016/j.heliyon.2023.e14234

Shafiei Nikabadi, M., Toghi, S., & Hakaki, A. (2021). A Combined Approach of FMEA and Gray Theory to Rank Aspects of Information Security Risk Management. *Business Intelligence Management Studies, 9*(34), 191–214. doi:10.22054/ims.2020.46866.1602. [In Persian]

Shiau, W.-L., Wang, X., & Zheng, F. (2023). What are the trend and core knowledge of information security? A citation and co-citation analysis. *Information & Management, 60*(3), 103774. doi:https://doi.org/10.1016/j.im.2023.103774

Shkarlet, S., Lytvynov, V., Dorosh, M., Trunova, E., & Voitsekhovska, M. (2020, 2020//). *The Model of Information Security Culture Level Estimation of Organization.* Paper presented at the Mathematical Modeling and Simulation of Systems, Cham.

Stanojević, M., & Izgarević, D. (2025). THE ROLE OF HUMAN RESOURCE MANAGEMENT IN ENHANCING CORPORATE INFORMATION SECURITY CULTURE. *MEGATREND REVIJA MEGATREND REVIEW*, 105.

Tahmasebi Limooni, S., & Fallah Kordabadi, M. (2019). IInvestigating the Situation of Information Security Architecture in Mazandaran Public Libraries Based on ISO / IEC 27002 Standard. *Digital and Smart Libraries Research, 6*(2), 35–50. doi:10.30473/mrs.2020.50639.1412

Talebi, H., & Taboli, H. (2024). Implementing a Structural-Interpretive Model for Information Security Management in Iranian Governmental Organizations: An Art-Islamic Approach. *Islamic Art Studies, 21*(56), 331–348. doi:10.22034/ias.2021.300790.1696

Varsos, D. S., Giannakou, S. A., & Assimakopoulos, N. A. (2018). A systems approach to information security for the twenty-first century organization. *Acta Europeana Systemica, 8*, 167–178.

vazife, z., Mahdi, M., & Vakili, N. (2019). Model for Feasibility Study and Effective Deployment of Information Security Management Systems Based on Meta-Synthesis Technique. *Business Intelligence Management Studies, 7*(26), 71–99. doi:10.22054/ims.2019.9717

Vedadi, A., Warkentin, M., Straub, D. W., & Shropshire, J. (2024). Fostering information security compliance as organizational citizenship behavior. *Information & Management, 61*(5), 103968. doi:https://doi.org/10.1016/j.im.2024.103968

Wagner, T. L. (2023). *Neutralization Techniques' Effect on US Employees' Intent to Violate Organizational Information Security Policy: A Quantitative Study*. Capella University,

Weng, W. (2024). A Beginner's Guide to Informatics and Artificial Intelligence. doi:https://doi.org/10.1007/978-981-97-1477-3_9

Yazdanmehr, A., Jawad, M., Benbunan-Fich, R., & Wang, J. (2024). The role of ethical climates in employee information security policy violations. *Decision Support Systems, 177*, 114086. doi:https://doi.org/10.1016/j.dss.2023.114086