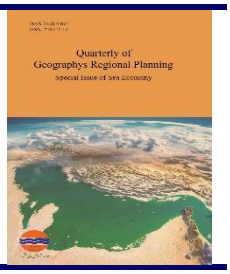
Iranian Association of Geopolitical

Geography (Regional Planning)

Winter 2024. Vol 14. Issue 57

ISSN (Print): 2228-6462 - ISSN (Online): 2783-2112

Journal Homepage: https://www.jgeoqeshm.ir/



Research Paper

Identifying the Factors and Components of the Information Technology Security Model with the Approach of Professional Ethics Policies of Employees in the Country's Municipalities

Mostafa Esfandiar[1], Mansour Esmaeilpour[*2], Reza Taghvaei[3], Behrooz Bayat[4]

1. PhD student in Information Technology Management, Department of Management, Hamedan Branch, Islamic Azad University, Hamedan, Iran.
2. Associate Professor, Computer Department, Hamedan Branch, Islamic Azad University, Hamedan, Iran.
3. Assistant Professor, Department of Management, Tuyserkan Branch, Islamic Azad University, Tuyserkan, Iran.
4. Assistant Professor, Department of Information Science and Epistemology, Hamedan Branch, Islamic Azad University, Hamedan, Iran.

ARTICLEINFO

PP: 122-145

Use your device to scan and read the article online

Keywords: *Ensuring the Security of Information Technology, Professional Ethics of Employees, Professional Ethics Policy*

Abstract

The main goal of this research is to identify the factors and components of information technology security with the approach of professional ethics policies of employees in the country's municipalities. This research is applied-developmental and exploratory in nature. The methodology of the research is qualitative and has been conducted using semi-structured interviews with experts. Sampling was done by snowball method from two groups of scientific-academic experts and executive experts and theoretical saturation was reached after 12 interviews. The data from the interviews were analyzed using Maxqda 2018 software and thematic analysis method. The findings of the research showed that among the variables examined in the current research, the average of information technology security based on professional ethics policies was equal to 2.97 and among its indicators, the structural index was the highest and the behavioral index was the highest. They had the lowest average. The results of qualitative data analysis show 6 dimensions (professional ethics, commitment and responsibility, creativity and innovation, human resource management, human resource performance and organization structure) and 22 organizational themes and 210 themes. It was the base. The results showed that success in providing information technology security in municipalities requires simultaneous attention to three contextual, behavioral and structural dimensions. It also shows that organizations that have been able to institutionalize the principles of professional ethics in their organizational culture, in case of security problems, have more ability to manage and control damages.

Citation: Esfandiar, M., Esmaeilpour, M., Taghvaei, R., Bayat, B. (2024). **Identifying the Factors and Components of the Information Technology Security Model with the Approach of Professional Ethics Policies of Employees in the Country's Municipalities.** Geography (Regional Planning), 14 (57), 122-145

DOI: 10.22034/jgeoq.2024.487991.4168

* **Corresponding author:** Mansour Esmailpour, **Email:** esmaeilpour@iauh.ac.ir

Extended Abstract

Introduction

With the advent of networks and easy access to the Internet, more information is being processed and transmitted through this platform, and more information is recorded and stored digitally and is being reproduced at a faster rate. Along with these changes, threats, destruction and theft of information have also increased, hence maintaining the security of the information exchange area is considered one of the most important goals of the development of information and communication technology. Information systems rely on hardware, software, data, controls, procedures and people in an organization. All of these elements require adequate management and effective management systems to protect the confidential information of the organizations involved, and these functions require special security controls to protect them. The life of organizations is closely related to their information systems. To solve a security problem, a company must use knowledge, technology and comprehensive organizational rules. Information technology security management is increasingly intertwined with professional ethics policies and emphasizes the need for ethical frameworks to guide cybersecurity actions. Ethical discussions in the organizational sphere show the difference between economic performance (revenues, costs, and profits) and social performance (the organization's obligations to others, both internal and external). Municipal employees have numerous ethical problems that affect the performance of the municipality, the privacy of citizens, and even national security. Employees may access and misuse confidential information of citizens for personal or commercial purposes. This information can include financial, personal, or even information related to municipal projects. Sharing confidential information with unauthorized persons, whether intentionally or unintentionally, can lead to information leakage. This can damage the reputation of the municipality and undermine the trust of citizens. The lack of appropriate monitoring systems and the lack of regular review of employee activities can provide opportunities for abuse for some individuals. Finally, the lack of an information security culture in the organization can cause employees not to realize the importance of this issue and not to take the necessary measures. Given that no study was found in this field that provides solutions to managers and employees in the field of ensuring information technology security based on professional ethics, it is necessary to mention the question here: what factors and components exist for ensuring information technology security with the approach of professional ethics policies for employees of the country's municipalities?

Methodology

This research is classified as applied-developmental research and, given its exploratory nature, seeks to analyze and explain in depth the factors and components of ensuring information technology security with a focus on professional ethics policies for employees in the country's municipalities. Given that the research topic is in the early stages of conceptualization, a qualitative approach using the content analysis method was chosen as the main research strategy.

Results and Conclusion

In the present era, when information technology plays a pivotal role in all areas of urban management, the issue of ensuring data and information security has become one of the fundamental challenges for municipalities. Municipalities, as non-governmental public institutions, deal with a huge volume of citizens' personal information, financial data, legal documents, and urban planning documents on a daily basis, and protecting them against cyber threats and possible abuses is a vital matter. In this regard, the role of the human factor, and in particular, the observance of professional ethics by employees, is doubly important. The present study aimed to identify the factors and components of ensuring information technology security with the approach of employee professional ethics policies in the country's municipalities. The findings of this study show that success in ensuring information security requires simultaneous attention to three contextual, behavioral, and structural dimensions. Previous studies show that continuous training in the field of professional ethics can reduce security risks by up to 60 percent and have been more successful in preventing security incidents. This study emphasizes that in order to achieve a desirable level of information technology security in municipalities, a comprehensive and integrated approach must be adopted in which, in addition to technical and technological aspects, special attention is paid to human and ethical dimensions. They have also all emphasized the pivotal role of professional ethics in the success of information

security programs. All of these studies, despite differences in the statistical population and methodology, have reached similar results regarding the pivotal role of professional ethics in ensuring information security. The ethics-based approach to information security management has become a competitive advantage, beyond an organizational requirement. Also, the alignment of results regarding the effect of professional ethics training on reducing security risks reveals the importance of investing in this area. Studies show that organizations that conduct regular training programs in the field of professional ethics have experienced a 60% reduction in security incidents. In addition, the alignment of results regarding the importance of a flexible and responsive organizational structure indicates the need to review traditional structures and move towards more agile models. These findings collectively confirm the three-dimensional approach (contextual, behavioral, and structural) of the present study, which has attempted to consider all aspects affecting information security with a comprehensive and integrated view.

In this regard, it is suggested that municipalities prepare the ground for improving the level of information security by formulating clear ethical policies, holding regular training courses, creating incentive systems for desirable security behaviors, and continuously monitoring employee performance. It is also essential that these policies are continuously reviewed and updated to keep pace with rapid technological developments and emerging threats. By identifying 22 components and 225 indicators in the form of three main dimensions, this research presents a comprehensive framework for managing information technology security in municipalities that can be a guide for managers and experts in this field. In order to improve the level of information technology security in municipalities and according to the findings of this research, the following practical suggestions are presented.

-Developing and implementing a comprehensive information security management system based on professional ethics by municipalities

-Holding continuous and targeted training courses focusing on the ethical aspects of information security for all organizational levels

-Adhering to ethical principles in the field of information security as one of the key performance indicators in the employee performance evaluation system

-Creating effective communication channels for reporting security incidents and supporting employees who report security violations

-Developing the organization's technical infrastructure in line with the latest security standards.

References

1. Akhavan, Fatemeh and Radfar, Reza. (2019). Presenting a model for monitoring information security maturity. Roshd Tehniqi Quarterly, 16(64): 1-10. [In Persian]
2. Akinsanya, M. O., Ekechi, C. C. and Okeke, C. D. (2024). Virtual private networks (vpn): a conceptual review of security protocols and their application in modern networks. Engineering Science & Technology Journal, 5(4), 1452-1472.
3. AlGhamdi, S, et al. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. Government Information Quarterly16 June 2022.
4. Chua, H.N., Ooi, J.S. and Herbland, A. (2021). The effects of different personal data categories on information privacy concern and disclosure. Computers & Security, 110, 102453.
5. De Zoysa, A.H.N. (2022). Inculcating Professional Ethics among Employees in the Workplace A Systematic Literature Review, International Journal of Multidisciplinary Studies (IJMS), Volume 9, Issue I.
6. Deh Dast, Naser. (1400). A study and identification of the components of professional ethics (a case study of Tehran Municipality). Afagh Humanities Monthly, 5(56), 1-17.
7. Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S. and Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: a review. Sensors, 23(3), 1151.
8. Dosti, Mehdi. (1402). Professional ethics in information technology. Two Monthly Journals of Management Engineering, 16(85), 37. [In Persian]
9. Eidi, Fatemeh; Kordi, Morad and Alizadeh Jorkouyeh, Ebrahim. (1402). Improving the performance of electronic banking by paying attention to information technology

capabilities, supply chain management methods and information security risk management. Journal of Modern Banking Studies, 6(18): 8-40. [In Persian]

10. Faramarzpour, Fatemeh and Faramarzpour, Mehdi. (1402). Investigating the effect of organizational culture on social responsibility and organizational commitment with the mediating role of professional ethics and strategic leadership behavior, a case study of Neyshabur Municipality employees. The 8th International Conference on Interdisciplinary Studies in Management and Engineering, University of Tehran.

11. Farayola, O. A., Olorunfemi, O. L. and Shoetan, P. O. (2024). Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal, 5(3), 606-615.

12. Ghamkhavari, Seyedeh Masoumeh; Nabinia, Alireza and Rasouli, Amir. (1403). The relationship between organizational commitment and organizational citizenship behavior: the mediating role of professional ethics. Ethics in Science and Technology, 144-150. [In Persian]

13. Haddadi Harandi, Ali Akbar; Valmohammadi, Chengiz and Salehi Sediqiani, Jamshid. (2019). Information Security Management in a Smart Organization, Bi-Quarterly Scientific and Research Journal of Crisis Management, Special Issue on Smartization, 33(25): 1-15. [In Persian]

14. Hadi, A., Miftachul, H., Novel, L. and Badlihisham, M. N. (2024). 2. Managing Professional-Ethical Negotiation for Cyber Conflict Prevention. International journal of cyber behavior, psychology, and learning, doi: 10.4018/ijcbpl.344022

15. Hakim, A. and Supriyatno, B. (2023). The Effect of Work Ethics and Employee Empowerment on Organizational Performance in Tebet District, South Jakarta Administrative City. International Journal of Education, Business and Economics Research (IJEBER), 3(4), 207-221

16. Hamidi Ashtiani, Saman. (2019). A study of strategic elements of information technology and its alignment with organizational business information security. The Fourth National and First International Conference on New Management and Organizational Models, Tehran. [In Persian]

17. Hilhorst, C., et al. (2022). Efficiency gains in public service delivery through information technology in municipalities. Government Information Quarterly16 June 2022.

18. Jha, J. and Singh, M. (2023). Who cares about ethical practices at workplace? A taxonomy of employees' unethical conduct from top management perspective. International Journal of Organizational Analysis, 31(2), 317-339

19. Kalantari, Reza; Moeini, Ali; Safari, Hossein and Arab Sorkh, Abuzar. (2020). Providing a conceptual framework for measuring the performance of information security service supply chains based on the meta-synthesis approach and the fuzzy Delphi method. Journal of Industrial Management, University of Tehran, 12(1): 24-46. [In Persian]

20. Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet of Things16 June 2021.

21. Khalifah Soltani, Heshmat; Taskhori Beheshti, Parisa and Chinichian Moghadam, Iman. (1400). The crisis of demoralization and the development of ethics in information technology professionals. The Eighteenth International Conference on Management, Tehran. [In Persian]

22. Mahmoudi Jabdaragh, Yaqoub; Pakmaram, Asgar; Abdi, Rasoul and Rezaei, Nader. (2013). Presenting a model for managing conflict and conflict in the accounting environment with emphasis on the components of professional ethics. Ethics in Science and Technology Quarterly, 17(1), 78-89. [In Persian]

23. Menbarrow Z. (2021). The Importance and Necessity of Professional Ethics in the Organization and the Role of Managers. Psychology and Behavioral Science International Journal, Volume 18, Issue 1, DOI: 10.19080/PBSIJ.2021.18.555979.

24. Moghimi Khorasani, A. (2014). The relationship between managers' leadership style and employees' professional ethics. Ethics in Science and Technology, 18(4), 192-196 [In Persian]

25. Mohammadi, Reza and Bastami, Hematollah. (2024). Modeling the causal relationship between organizational virtue and professional ethics of employees of the General Directorate of Sports and Youth of Kermanshah Province with the mediating role of strategic human resource management.

Studies on organizational behavior management in sports. [In Persian]

26. Navdeep., Akshay, G., Muskan., Vaibhav, and Sharma. (2023). The Role of Ethics in Developing Secure Cyber-Security Policies. doi: 10.52783/tjjpt.v43.i4.2346

27. Ning, Y. (2022). Information security challenge of modern society. Vestnik Ûžno-Ural′skogo gosudarstvennogo universiteta, 14(2), 65-70, https://www.doi.org/10.14529/ped220206.

28. Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299-1323.

29. Rao, P. S., Krishna, T. G. and Muramalla, V. S. S. R. (2023). Next-gen cybersecurity for securing towards navigating the future guardians of the digital realm. International Journal of Progressive Research in Engineering Management and Science (IJPREMS) Vol, 3, 178-190.

30. Saha, P. (2018). Government e-service delivery: identification of success factors from citizens' perspective (Doctoral dissertation, Luleå tekniska universitet).

31. Salahshouri, Farhad; Rigi, Mohsen and Kaykha, Somayeh. (1401). A study and explanation of data security. The Second International Conference on Electrical, Computer and Mechanical Engineering. [In Persian]

32. Saraswat, A. K. and Meel, V. (2022). Protecting data in the 21st century: Challenges, strategies and future prospects. Information technology in industry, 10(2), 26-35

33. Sarwari, A. Sh. and ul Haq, A., (2023). International professional ethics. The Islamic Culture" As-Saqafat-ul Islamia" Research Journal-Sheikh Zayed Islamic Centre, University of Karachi, 48(2), 17-33, http://theislamicculture.com/index.php/tis/article/view/933.

34. Shakeri, Mohammad Javad; Mokhtar, Aida and Rastegari, Behnam. (1404). Application of blockchain technology in ensuring the security of judicial electronic information. Journal of Interdisciplinary Studies of Jurisprudence, 5(2), 1-17. [In Persian]

35. Siewert, W. and Udani, A. (2016). Missouri municipal ethics survey: Do ethics measures work at the municipal level?. Public Integrity, 18(3), 269-289.

36. Sohrabi, Shahla; Shams, Hossein and Azizinejad, Hossein. (1400). The role of Islamic professional ethics in the success of Iranian project-based organizations. Journal of Management Sciences Research, 3(7): 1-15. [In Persian]

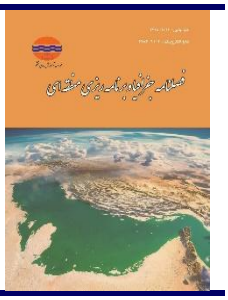
37. Steen, M. E. (2023). Ethics as a Participatory and Iterative Process. Communications of the ACM, 66(5), 27-29, https://www.doi.org/10.1145/3550069.

38. Stergiou, C., Psannis, K. E., Kim, B. G. and Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.

39. Taherirad, Zahra and Veisi, Parham. (1401). Implementation of SOC Security Operations Center in Shiraz Municipality Information and Communication Technology Organization. 15th International Conference on Information Technology, Computers and Telecommunications. [In Persian]

40. Vazifeh, Zahra; Mehdi, Mohammad and Vakili, Nadia. (2018). A model for assessing the feasibility and effective establishment of an information security management system based on the meta-synthesis method. Smart Business Management Studies, 7(26), 71-99. [In Persian]

41. Yazdanmehr, A., Li, Y. and Wang, L. (2023). Employee responses to information security related stress: Coping and violation intention. Information Systems Journal, 33(3), 598-639, https://doi.org/10.1111/isj.12417.



فصلنامه جغرافیا (برنامه ریزی منطقه ای)

دوره ۱۴، شماره ۵۷، زمستان ۱۴۰۳

شاپا چاپی: ۶۴۶۲- ۲۲۲۸ شاپا الکترونیکی: ۲۱۱۲ -۲۷۸۳

Journal Homepage: https://www.jgeoqeshm.ir/

انجمن ژئوپلیتیک ایران

مقاله پژوهشی

شناسایی عوامل و مؤلفه‌های مدل تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور

مصطفی اسفندیار– دانشجوی دکتری مدیریت فناوری اطلاعات، گروه مدیریت، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران.

منصور اسماعیل‌پور*– دانشیار، گروه کامپیوتر، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران.

رضا تقوایی– استادیار، گروه مدیریت، واحد تویسرکان، دانشگاه آزاد اسلامی، تویسرکان، ایران.

بهروز بیات– استادیار، گروه علم اطلاعات و دانش شناسی، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران.

اطلاعات مقاله

شماره صفحات: ۱۴۵-۱۲۲

از دستگاه خود برای اسکن و خواندن مقاله به صورت آنلاین استفاده کنید

واژه‌های کلیدی:

تأمین امنیت فناوری اطلاعات، اخلاق حرفه¬ای کارکنان، خط‌مشی اخلاق حرفه‌ای.

چکیده

هدف اصلی این پژوهش، شناسایی عوامل و مؤلفه‌های تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور می‌باشد. این پژوهش از نوع کاربردی-توسعه‌ای و با ماهیت اکتشافی انجام شده است. روش‌شناسی پژوهش کیفی بوده و با استفاده از مصاحبه‌های نیمه‌ساختاریافته با خبرگان انجام گرفته است. نمونه‌گیری به روش گلوله برفی از دو گروه خبرگان علمی- دانشگاهی و خبرگان اجرایی صورت پذیرفت و پس از انجام ۱۲ مصاحبه به اشباع نظری رسید. داده‌های حاصل از مصاحبه‌ها با استفاده از نرم‌افزار Maxqda 2018 و به روش تحلیل مضمون مورد تجزیه و تحلیل قرار گرفت. یافته‌های حاصل از پژوهش نشان داد در بین متغیرهای مورد بررسی در پژوهش حاضر، میانگین تأمین امنیت فناوری اطلاعات مبتنی بر خط¬مشی‌های اخلاق حرفه¬ای برابر با ۲/۹۷ به دست آمد و در بین شاخص‌های آن، شاخص ساختاری بیشترین میانگین و شاخص رفتاری کمترین میانگین را داشتند. نتایج حاصل از تحلیل کیفی داده¬ها نشان دهنده¬ی ۶ بعد (اخلاق حرفه¬ای، تعهد و مسئولیت¬پذیری، خلاقیت و نوآوری، مدیریت منابع انسانی، عملکرد منابع انسانی و ساختار سازمان) و ۲۲ مضمون سازمان¬دهنده و ۲۱۰ مضمون پایه بود. نتایج نشان داد که موفقیت در تأمین امنیت فناوری اطلاعات در شهرداری‌ها، نیازمند توجه همزمان به سه بعد زمینه‌ای، رفتاری و ساختاری است. در بعد زمینه‌ای، عواملی چون احترام به حریم خصوصی شهروندان، رعایت انصاف در دسترسی به اطلاعات و پایبندی به ارزش‌های اجتماعی اهمیت دارد. در بعد رفتاری، مؤلفه‌هایی همچون مدیریت عملکرد، تصمیم‌گیری‌های اخلاقی و رفتار سازمانی نقش کلیدی ایفا می‌کنند و در بعد ساختاری، عناصری مانند طراحی ساختار سازمانی منعطف، تدوین قوانین شفاف و ایجاد زیرساخت‌های فنی مناسب مورد توجه قرار می‌گیرند. نتایج همچنین نشان می‌دهد که سازمان‌هایی که توانسته‌اند اصول اخلاق حرفه‌ای را در فرهنگ سازمانی خود نهادینه کنند، در صورت بروز مشکلات امنیتی، توانایی بیشتری در مدیریت و کنترل آسیب‌ها داشته‌اند.

استناد: اسفندیار، مصطفی؛ اسماعیل پور، منصور؛ تقوایی، رضا؛ بیات، بهروز (۱۴۰۳). **شناسایی عوامل و مؤلفه‌های مدل تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور.** فصلنامه جغرافیا (برنامه‌ریزی منطقه‌ای)، ۱۴ (۵۷). صص: ۱۴۵-۱۲۲

DOI: 10.22034/jgeoq.2024.487991.4168

* **نویسنده مسئول:** منصور اسماعیل‌پور، **پست الکترونیکی:** esmaeilpour@iauh.ac.ir

مقدمه

در عصر حاضر اگر مردم یک کشور در مسیر بلوغ فکری قرار گیرند، می‌توانند به توسعه پایدار و همه جانبه دست یابند و این امر تنها با تسهیل استفاده و تبادل دانش و اطلاعات امکان پذیر خواهد بود. توجه به آن برای تسهیل زندگی شهروندان و تحقق اهداف عالی کشور با استفاده از امکانات فناوری اطلاعات به شدت احساس می‌شود. با ظهور شبکه ها و دسترسی آسان به اینترنت، بیشتر اطلاعات از طریق این بستر در حال پردازش و انتقال است و بیشتر اطلاعات به صورت دیجیتالی ضبط و ذخیره شده و با سرعت بیشتری تکثیر می‌شوند. همزمان با این تغییرات، تهدیدات، تخریب و سرقت اطلاعات نیز افزایش یافته است، بنابراین حفاظت و امنیت اطلاعات به یکی از مهمترین مشکلات عصر حاضر تبدیل شده است (وظیفه و همکاران، ۱۳۹۷). بحث امنیت در دنیای تبادل داده‌ها، جایگاه و اهمیت ویژه‌ای دارد، امنیت به قدری حیاتی و مهم می‌باشد که در تدوین قانون آیین دادرسی الکترونیکی، قانونگذار چند ماده را به مقوله امنیت اختصاص داده و برای نقض کنندگان آن نیز مجازات‌هایی تعیین نموده است (شاکری و همکاران، ۱۴۰۴).

بسیاری از مراکز و مؤسسات دولتی و خصوصی، بانک‌ها، شرکت‌ها و آژانس‌ها، مراکز آموزشی، علمی، ترویجی و اطلاع‌رسانی از سیستم‌های اطلاعاتی و فناوری‌های اطلاعاتی پیچیده در سازمان خود برای انجام وظایف و وظایف خود استفاده می‌کنند. بسیاری از ویژگی‌های آن؛ سهولت انتقال اطلاعات، سرعت انتقال اطلاعات، ذخیره حجم زیاد اطلاعات، کاهش هزینه، صرفه جویی در زمان، قابلیت اطمینان و دقت در انجام کار و غیره می‌باشد. فناوری اطلاعات با کمک علوم مختلف توانسته است در مدت زمان کوتاهی اطلاعات مهمی را در اختیار انواع افراد قرار دهد. این فناوری چندین کشور را در سراسر جهان به هم متصل می‌کند (دیرانی[1] و همکاران، ۲۰۲۳). اما اگر هنگام تماشای پیشرفت و یادگیری او به ایمنی او توجه نشود، می تواند بسیار خطرناک باشد. از سوی دیگر، با بهبود فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب پذیری توانایی تبادل اطلاعات افزایش یافته و روش‌های انجام تهدیدات مذکور دشوارتر می‌شود (نینگ[2]، ۲۰۲۲). از این رو حفظ امنیت حوزه تبادل اطلاعات یکی از مهمترین اهداف توسعه فناوری اطلاعات و ارتباطات محسوب می‌شود. محققان بر این باورند که اکثر سازمان‌ها صرف نظر از خطرات این فناوری، هزینه‌های زیادی را صرف توسعه فناوری اطلاعات می‌کنند و اغلب با اجرای استراتژی‌های موقتی مانند نصب آنتی ویروس و فایروال سعی در حفاظت از اطلاعات دارند. در صورتی که آسیب بیشتری ببینند اما متأسفانه این روش را ادامه می‌دهند. سیستم‌های اطلاعاتی بر سخت افزار، نرم افزار، داده‌ها، کنترل‌ها، رویه‌ها و افراد در یک سازمان متکی هستند. تمامی این عناصر نیازمند مدیریت کافی و سیستم‌های مدیریتی مؤثر برای محافظت از اطلاعات محرمانه سازمان‌های درگیر هستند و این کارکردها نیازمند کنترل‌های امنیتی ویژه هستند تا از آنها محافظت شود (عیدی و همکاران، ۱۴۰۲). سیستم‌های اطلاعاتی و برنامه‌های کاربردی یک سازمان اغلب سیستم‌های پیچیده‌ای هستند که بسیاری از وظایف را در داخل سازمان پوشش می‌دهند. از آنجایی که سازمان معمولاً وابستگی زیادی به این سیستم‌ها دارد، هر نوع عاملی که عملکرد آنها را مختل کند می تواند آسیب‌های جدی و جبران ناپذیری به سازمان وارد کند. مسائل امنیتی یک مشکل رایج در سیستم‌های اطلاعاتی است و با توجه به استفاده از سیستم‌های اطلاعاتی و برنامه‌های کاربردی در بسیاری از سازمان‌ها، مقوله امنیتی این سیستم‌ها از اهمیت بالایی برخوردار است (ساها[3] و همکاران، ۲۰۱۸) حیات سازمان‌ها ارتباط تنگاتنگی با سیستم‌های اطلاعاتی آنها دارد. سیستم‌های اطلاعاتی همیشه در معرض خطر سرقت داده‌ها، تغییر داده‌ها و قطع سرویس هستند. برای حل یک مشکل امنیتی، یک شرکت باید از دانش، فناوری و قوانین جامع سازمانی استفاده کند و اطمینان حاصل کند که شرکت نه تنها بر راه حل‌های فنی تمرکز دارد، بلکه از آنها نیز استفاده می‌کند (یزدان مهر و همکاران، ۲۰۲۳). معرفی موفقیت‌آمیز فناوری‌های جدید به دولت این امکان را می‌دهد که خدمات عمومی مؤثرتری به شهروندان ارائه کند و با توجه به اهمیت نقش مدیریت امنیت فناوری اطلاعات در حفاظت از اطلاعات سازمان، یکی از عواملی است که می‌تواند منجر به تغییر سازمانی شود، ارزش‌های اخلاقی است که اعمال می شود؛ اینها سیاست‌ها و

1. Dhirani
2. Ning
3. Saha

برنامه‌های مدیریت امنیت اطلاعات هستند. بنابراین اهمیت تحقیقات گسترده در زمینه اخلاق حرفه‌ای و کسب و کار در حوزه مدیریت امنیت فناوری اطلاعات مشخص می‌شود (استرگیو[1] و همکاران، ۲۰۱۸).

مدیریت امنیت فناوری اطلاعات به طور فزاینده‌ای با سیاست‌های اخلاق حرفه‌ای در هم آمیخته است و بر نیاز به چارچوب‌های اخلاقی برای هدایت اقدامات امنیت سایبری تأکید می‌کند. این ادغام برای توسعه استراتژی‌های امنیت سایبری انعطاف‌پذیر که نه تنها از داده‌ها محافظت می‌کند، بلکه از استانداردهای اخلاقی در تعاملات دیجیتالی نیز حمایت می‌کند، حیاتی است. بخش‌های بعدی جنبه‌های کلیدی این رابطه را بیان می‌کند (هادی و همکاران، ۲۰۲۴). چارچوب‌های اخلاقی برای شکل‌دهی سیاست‌های امنیت سایبری، پرداختن به معضلاتی که از پیشرفت‌های سریع فناوری ناشی می‌شوند، ضروری هستند (ناودیپ[2] و همکاران، ۲۰۲۳). گزارش منلو و اصول مبتنی بر حقوق، دستورالعمل‌های اخلاقی اساسی را برای اقدامات امنیت سایبری ارائه می‌کنند (لیو و کریستن[3]، ۲۰۲۰). الزامات اخلاقی شامل تضمین حریم خصوصی، پاسخگویی و شفافیت در اقدامات امنیت سایبری است (ناودیپ و همکاران، ۲۰۲۳).

همانطور که در مطالعه اسفندیار و همکاران (۱۴۰۲) گفته شده در صورت پیروی نکردن کارکنان از خط‌مشی و اصول اخلاقی کارکنان می‌تواند منجر به نقص امنیت داده‌ها یا سیستم‌ها منجر شود. راهنمایی و نظارت کردن بر رفتارها می‌تواند ساز و کارهای کارکنان را به آنها یادآوری کرده و به سمت مسیر صحیح رفتاری آنها را هدایت کند. همچنین در بررسی که توسط باقریان فر و همکاران (۱۳۹۷) صورت گرفت این مطلب بیان شد که بین استفاده از ماهواره و اینترنت توسط کارکنان و اخلاق حرفه‌ای آنها رابطه معکوس وجود دارد و هر چقدر افراد از این فناوری‌ها استفاده کنند اخلاق حرفه‌ای در آنها کمتر می‌شود.

اخلاق به طور ساده و خلاصه شناخت صحیح از ناصحیح است و انجام امور صحیح و ترک امور ناصحیح می‌باشد (مقیمی خراسانی، ۱۴۰۲). به عنوان چارچوبی برای ارزیابی اقدامات و تصمیمات، هدایت افراد و جوامع در تعاملاتشان عمل می‌کند. اخلاق ثابت نیست. با هنجارهای اجتماعی و زمینه‌های فرهنگی تکامل می‌یابد و نیاز به تأمل مداوم و اصلاح معیارهای اخلاقی دارد. اخلاق شامل استانداردهای مستدلی است که رفتار انسانی، از جمله وظایف مربوط به حقوق و منافع اجتماعی را تجویز می‌کند (ساروای و هاگ[4]، ۲۰۲۳). غالباً به عنوان یک کد اخلاقی که توسط افراد یا گروه‌ها اعمال می‌شود، تعریف می‌شود که منعکس‌کننده باورهایی درباره رفتار قابل قبول است. اخلاق یک فرآیند مشارکتی و تکراری است که مستلزم تحقیق و بررسی مداوم در جوامع است (استین[5]، ۲۰۲۳). مراد از اخلاق، شاخص‌ها و ویژگی‌های اخلاقی است که جامعه باید در رابطه با مقررات فنی و اخلاقی آن‌ها را رعایت کند و تبعیت جامعه از آن‌ها پیامدهای منفی دارد. یکی از کارشناسان معتقد است که بسیاری از موارد اخلاقی زمانی به وجود می‌آیند که فردی بخواهد نوعی خوبی را در کار نشان دهد، اما از او خواسته می‌شود به جای اینکه بخواهد فردی کامل و خوب باشد، فقط عملکرد فنی کافی از خود نشان دهد، مشکلات اخلاقی شروع می‌شود. از جمله مؤلفه‌های اخلاق حرفه‌ای می‌توان به این موارد اشاره کرد: ویژگی‌های شخصیتی، مهارت‌ها، مأموریت و مأموریت‌ها، استراتژی، فرهنگ سازمانی، سبک مدیریت، ارزیابی و نظارت، عوامل انگیزشی، ساختار سازمانی و مدیریت منابع انسانی (محمودی جبدرق و همکاران، ۱۴۰۱). اخلاق حرفه‌ای به اصول و معیارهای اخلاقی اطلاق می‌شود که رفتار را در زمینه حرفه‌ای هدایت می‌کند. این شامل ارزش‌ها و هنجارهایی است که بر نحوه رفتار افراد در محیط‌های کاری خود حاکم است. اخلاق حرفه‌ای به تعاملات سازنده انسانی در محیط کار کمک می کند و به افراد آسیب دیده در محیط کار کمک می‌کند (غمخوار و همکاران، ۱۴۰۳). امروزه بحث اخلاقیات یکی از مباحث عمده علم مدیریت گردیده است. از اینرو است که بحث اخلاقیات نقش مهم و تعیین‌کننده‌ای دارد. کشورها به این بلوغ فکری رسیده‌اند که بی‌اعتنایی به مسائل اخلاقی و فرار از مسئولیت‌ها و تعهدات اجتماعی به از بین رفتن موسسه و سازمان می‌انجامد؛ به همین دلیل بسیاری از مؤسسات و سازمان‌های موفق، برای تدوین استراتژی اخلاقی احساس نیاز کرده و به این باور رسیده‌اند که باید در سازمان یک فرهنگ مبتنی بر اخلاق رسوخ کند. از این‌رو کوشیده‌اند، به تحقیقات درباره اخلاق حرفه‌ای جایگاه ویژه‌ای ببخشند.

1. Stergiou
2. Navdeep
3 Loi & Christen
4. Sarwari & Haq
5. Steen

در واقع، اخلاق حرفه‌ای به عنوان دانش حل مشکلات اخلاقی سازمان و توضیح تعهدات و مسئولیت‌های اخلاقی سازمان عمل می‌کند (محمدی و بسطامی، ۲۰۲۴).

اخلاق حرفه‌ای برای پرورش فرهنگ اخلاقی قوی در سازمان ها بسیار مهم است. این به ایجاد اعتماد، مسئولیت پذیری و صداقت در بین کارکنان کمک می‌کند که برای کار تیمی موثر و موفقیت سازمانی ضروری است. اخلاق حرفه‌ای به طور قابل توجهی بر عملکرد کلی سازمان تأثیر می‌گذارد. بر فرآیندهای تصمیم گیری تأثیر می‌گذارد و فرهنگ سازمانی را شکل می‌دهد و در نهایت بر رفتار و عملکرد کارکنان تأثیر می‌گذارد. پرورش فرهنگ اخلاقی در شرکت‌ها نه تنها موجب تعیین استانداردهای اخلاقی می‌شود بلکه منجر به تشویق کارکنان به رعایت این استانداردها در فعالیت‌های روزانه نیز شده است. نگرش کارکنان نقش حیاتی در اخلاق محیط کار دارد. نگرش مثبت نسبت به رفتار اخلاقی می‌تواند جو اخلاقی یک سازمان را تقویت کند، در حالی که نگرش‌های منفی می‌تواند آن را تضعیف کند (زویسا[1]، ۲۰۲۲).

امروزه رعایت اخلاق حرفه‌ای توسط مدیران یکی از مهم‌ترین متغیرهای موفقیت سازمان‌ها محسوب می‌شود. در دهه گذشته مدیران سازمان‌ها بیش از هر زمان دیگری به اهمیت تزریق اخلاق حرفه‌ای به شریان‌های حیاتی سازمان‌ها پی برده‌اند و اکنون به خوبی می‌دانند که جوهره اخلاق پایداری سازمان و دستیابی به اهداف نهایی آنهاست. یکی از اساسی‌ترین اصول برای ایجاد ارتباط سالم و مؤثر در بین کارکنان سازمان‌ها، رعایت اصول اخلاق حرفه‌ای توسط مدیران سازمان‌ها است. در حال حاضر اطلاعات یک منبع استراتژیک و یک قابلیت کلیدی است که سایر عناصر مهم امنیت اطلاعات اعم از فرآیندها و پرسنل را در بر می‌گیرد و علاوه بر تضمین امنیت اطلاعات، باید به محیط اخلاقی حاکم بر سازمان نیز توجه ویژه ای داشت، زیرا در صورتی که اخلاق حرفه‌ای کارکنان به سازمان متصل باشد، آنها می‌توانند بهتر از اطلاعات سازمان و مسائل امنیتی آن محافظت کنند. از این رو موضوع امنیت اطلاعات و اخلاق حرفه‌ای کارکنان برای اطمینان از استفاده صحیح از این منبع در دستور کار دولت‌ها قرار گرفته است. اهداف اصلی ترویج اخلاق در فناوری اطلاعات مانند احترام واقعی و بی قید و شرط به افراد، آزادی فردی، عدالت اجتماعی و قابلیت اطمینان است (دوستی، ۱۴۰۲).

بحث‌های اخلاقی در حوزه سازمانی تفاوت بین عملکرد اقتصادی (درآمدها، هزینه ها و سود) و عملکرد اجتماعی (تعهدات سازمان در قبال دیگران در داخل و خارج) را نشان می‌دهد. اگرچه کشور دارای میراث تاریخی، تمدنی، فرهنگی و دینی روشن و ارزشمندی است، اما در افق کنونی آن، وقتی با کشورهای صنعتی غرب و حتی برخی جوامع مترقی مقایسه می‌شود، نسبت به شکوه تاریخی خود در توسعه اخلاق حرفه‌ای وضعیت مناسبی در صورتی که تاریخ فرهنگی و دینی کشور دارای گنج‌های ارزشمندی از میراث گران‌بهای خود در این زمینه می‌باشد. با توجه به این سرمایه‌ها و گذشت‌ها که اخلاق محور تربیت و عمل، اشتغال افراد و جامعه و حمایت و امداد است که منشأ قدرت پویای جامعه اسلامی و ایرانی بوده است، اما جامعه امروز از فقدان یا نبود پرسش‌های اخلاقی در تجارت رنج می‌برد (فرامرزپور، ۱۴۰۲). پایبندی به اخلاق حرفه‌ای نشان دهنده شخصیت یک فرد در یک سازمان است و این اخلاق حرفه‌ای است که باعث ارتقای مطلوب فرد در جامعه و در بین همکاران می‌شود. در این چارچوب اخلاق حرفه‌ای، نقش افراد در جامعه نمایان می‌شود و افراد نسبت به یکدیگر بیشتر جهت گیری می‌کنند. افزایش ارتباطات اجتماعی بین افراد مجموعه‌ای از استانداردهای اخلاقی و رفتار درونی را بین کارکنان و مدیران ایجاد می‌کند و همچنین نقش مهمی در انجام وظایف اداری و غیر اداری مربوط به مشتریان دارد. اخلاق حرفه‌ای محرک‌های زیادی را تحریک می‌کند و بسیاری از ناهنجاری‌ها را از بین می‌برد. ارزش‌های حرفه‌ای اعمال شده در یک سازمان با اخلاق حرفه‌ای مرتبط است. کارکنانی که دارای اخلاق کاری و ارزش‌ها و باورهای اخلاقی صحیح هستند، به این باور خواهند رسید که اخلاق کاری برای رشد فکری و معنوی آنها ضروری است (ده دست، ۱۴۰۰).

کارکنان شهرداری مشکلات اخلاقی متعددی دارند که این مشکلات بر عملکرد شهرداری، حریم خصوصی شهروندان و حتی امنیت ملی تاثیر دارد. کارکنان ممکن است به اطلاعات محرمانه شهروندان دسترسی پیدا کنند و از آن برای اهداف شخصی یا تجاری سوءاستفاده کنند. این اطلاعات می‌تواند شامل اطلاعات مالی، شخصی یا حتی اطلاعات مربوط به پروژه‌های شهری باشد.

1. Zoysa

به اشتراک‌گذاری اطلاعات محرمانه با افراد غیرمجاز، چه به صورت عمدی و چه به صورت سهوی، می‌تواند منجر به نشت اطلاعات شود. این امر می‌تواند به شهرت شهرداری آسیب رسانده و اعتماد شهروندان را سلب کند. در برخی موارد، کارکنان ممکن است با انگیزه‌های مختلف اقدام به هک کردن سیستم‌های شهرداری کنند. این عمل می‌تواند به اختلال در خدمات شهری، سرقت اطلاعات و حتی اخاذی منجر شود. همچنین استفاده غیرمجاز از نرم‌افزارهای رایانه‌ای می‌تواند به شهرداری خسارات مالی وارد کند و همچنین از نظر اخلاقی قابل توجیه نیست. کارکنان ممکن است با انگیزه‌های مختلف اقدام به تغییر یا حذف اطلاعات کنند. این عمل می‌تواند به ایجاد سردرگمی، اتخاذ تصمیمات اشتباه و حتی ایجاد خسارات مالی منجر شود. این مسائل و مشکلات به دلایل مختلفی می‌تواند رخ دهد. عدم آگاهی کارکنان از اصول امنیت اطلاعات و نبود آموزش‌های کافی در این زمینه می‌تواند منجر به بروز خطاهای انسانی شود. به علاوه نبود سیستم‌های نظارتی مناسب و عدم بررسی منظم فعالیت‌های کارکنان می‌تواند فرصت سوءاستفاده را برای برخی افراد فراهم کند. فشار کاری زیاد و عدم تعادل بین کار و زندگی شخصی نیز می‌تواند منجر به کاهش تمرکز و افزایش احتمال بروز خطا شود. در نهایت نبود فرهنگ امنیت اطلاعات در سازمان می‌تواند باعث شود که کارکنان به اهمیت این موضوع پی نبرند و اقدامات لازم را انجام ندهند. با توجه به اینکه مطالعه ای که در این زمینه راهکارهایی را به مدیران و کارکنان در زمینه تامین امنیت فناوری اطلاعات مبتنی بر اخلاق حرفه ای ارائه دهد یافت نشد بنابراین ذکر این پرسش در اینجا ضروری است که چه عوامل و مؤلفه‌هایی برای تامین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان شهرداری‌های کشور وجود دارد؟

مبانی نظری پژوهش

گذار سریع جوامع به عصر اطلاعات، موجب گسترش چشمگیر نظام‌های اطلاعاتی و خدمات مرتبط با آن گردیده و این تحول، به ظهور نسل نوینی از سازمان‌ها انجامیده است که از آن‌ها با عنوان سازمان‌های نوین یا سازمان‌های دانش‌محور یاد می‌شود (آکین سانیا و همکاران، ۲۰۲۴).

در عصر کنونی که شبکه‌های دیجیتال به‌طور گسترده‌ای در هم تنیده شده‌اند، مسئله صیانت از حریم شخصی و ایمن‌سازی اطلاعات به یکی از چالش‌های اساسی برای افراد، نهادها و حکومت‌ها تبدیل گشته است (فرایولا[1] و همکاران، ۲۰۲۴). مفهوم حفظ حریم خصوصی به معنای پاسداری از داده‌های حساس در مقابل هرگونه سوءاستفاده، دسترسی غیرمجاز و افشای ناخواسته است و این اطمینان را ایجاد می‌کند که صاحبان اطلاعات، اختیار کامل بر داده‌های شخصی خود دارند (چوآ[2] و همکاران، ۲۰۲۱).

امنیت اطلاعات دربرگیرنده مجموعه تدابیری است که از تمامیت، محرمانگی و دسترس‌پذیری داده‌ها در برابر مخاطرات گوناگون همچون تهاجمات سایبری، نشت اطلاعات و اقدامات خرابکارانه محافظت می‌کند (کوآچ[3] و همکاران، ۲۰۲۲). در حیطه فناوری اطلاعات که با انبوهی از تولید، ذخیره‌سازی و انتقال داده‌ها روبرو هستیم، اطمینان از برقراری امنیت و راهکارهای حفاظتی اهمیت ویژه‌ای می‌یابد (راو[4] و همکاران، ۲۰۲۳). این سازوکارهای امنیتی علاوه بر حفاظت از اطلاعات حساس، موجب تقویت اعتماد متقابل میان سازمان‌ها و مشتریان، رعایت الزامات قانونی و کاهش مخاطرات مالی و حیثیتی ناشی از نشت اطلاعات می‌شود. توسعه روزافزون فناوری‌های دیجیتال و رشد نمایی حجم داده‌ها، ضرورت حفاظت از اطلاعات در فضای دیجیتال را دوچندان کرده است (ساراسوات و میل[5]، ۲۰۲۲). تامین امنیت تنها محدود به جنبه‌های فنی نیست؛ بلکه تدوین و استانداردسازی سیاست‌های نظارتی و ایجاد رویه‌های صحیح نیز در ارتقای سطح امنیت اطلاعات نقش بسزایی دارد. امروزه مباحث امنیت اطلاعات ابعاد تازه‌ای یافته و در صدر اولویت‌های تمامی نهادها از جمله شهرداری‌ها قرار گرفته است (جدیدی، ۱۳۹۸). یکی از عوامل کلیدی در تضمین امنیت سازمانی، پایبندی کارکنان به اصول اخلاق حرفه‌ای است. این اصول باید توسط کارمندان به عنوان خدمتگزاران جامعه درک و درونی شود تا بتوانند سازگاری مطلوبی با محیط سازمانی و اجتماعی داشته باشند (حکیم و سوپریاتنو[6]، ۲۰۲۳). اخلاق حرفه‌ای را می‌توان توانمندی کارکنان

1. Farayola
2 Chua
3 Quach
4 Rao
5 Saraswat & Meel
6 Hakim & Supriyatno

در انجام مسئولیت‌ها همراه با صداقت، نظم، همکاری، آینده‌نگری، جدیت، دوراندیشی و احترام به زمان تعریف کرد که با نگرش بهبود مستمر همراه است (جها و سینگ[1]، ۲۰۲۳).

پژوهش‌ها نشان می‌دهد که تعهد کارکنان به اصول اخلاق حرفه‌ای، منجر به کاهش چشمگیر تخلفات سازمانی شده و از نقض قوانین و مقررات جلوگیری می‌کند که این امر به نوبه خود، حفاظت از داده‌های حیاتی سازمان را تضمین می‌نماید (سیورت و اودانی[2]، ۲۰۱۶).

روش پژوهش

این پژوهش در زمره تحقیقات کاربردی-توسعه‌ای قرار می‌گیرد و با توجه به ماهیت اکتشافی آن، به دنبال واکاوی و تبیین عمیق عوامل و مؤلفه‌های تأمین امنیت فناوری اطلاعات با محوریت خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور می‌باشد. نظر به اینکه موضوع پژوهش در مراحل اولیه مفهوم‌پردازی قرار دارد، رویکرد کیفی با استفاده از روش تحلیل مضمون به عنوان استراتژی اصلی پژوهش انتخاب گردید.

در گام نخست، با مطالعه عمیق ادبیات نظری و پیشینه تجربی موضوع، چارچوب مفهومی اولیه تدوین شد. سپس به منظور شناسایی و استخراج مؤلفه‌های کلیدی، از مصاحبه‌های نیمه‌ساختاریافته با خبرگان بهره گرفته شد. جامعه آماری پژوهش شامل دو گروه از متخصصان بود: الف) خبرگان دانشگاهی با تخصص در حوزه‌های مدیریت فناوری اطلاعات، امنیت سایبری و اخلاق حرفه‌ای و ب) مدیران و کارشناسان ارشد شهرداری‌ها با تجربه اجرایی در زمینه موضوع پژوهش.

نمونه‌گیری با استفاده از رویکرد زنجیره‌ای (گلوله برفی) آغاز و تا رسیدن به اشباع نظری ادامه یافت. در مجموع ۱۲ مصاحبه عمیق انجام شد که در آن هیچ داده یا مفهوم جدیدی که منجر به شناسایی عوامل و مؤلفه‌های گردد، حاصل نشد.

برای تضمین روایی و پایایی پژوهش، اقدامات متعددی صورت پذیرفت:

۱. انتخاب مشارکت‌کنندگان با معیارهای دقیق تخصصی و تجربی
۲. تحلیل و تفسیر داده‌ها توسط پژوهشگر با تجربه در روش‌های کیفی و آشنایی عمیق با حوزه موضوعی
۳. نظارت و راهنمایی مستمر توسط اساتید متخصص در پژوهش‌های کیفی
۴. مستندسازی دقیق و شفاف فرآیند پژوهش
۵. تصریح سوگیری‌های احتمالی پژوهشگر
۶. رعایت ملاحظات اخلاقی شامل اخذ رضایت آگاهانه و حفظ محرمانگی
۷. ادامه فرآیند جمع‌آوری داده‌ها تا حصول اطمینان از اشباع نظری

تحلیل داده‌ها با استفاده از روش تحلیل مضمون و طی سه مرحله کدگذاری باز، محوری و انتخابی انجام شد. نتایج این تحلیل منجر به شناسایی مضامین اصلی و فرعی و در نهایت شناسایی عوامل و مؤلفه‌های تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان در این پژوهش گردید.

یافته‌های پژوهش

جهت بررسی پایایی این پژوهش، از ضریب کاپا استفاده شد. از بر اساس مقالات به دست آمده شاخص کاپا برابر با مقدار ۰.۷۸ به دست آمد که نشان دهنده اعتبار کدهای استخراج شده بود که در جدول ۱ نشان داده شده است.

جدول ۱. ضریب توافق کاپا

1 Jha & Singh
2 Siwert & Odani

شرح		مقدار	خطای انحراف	تقریب آماره تی	سطح معنی داری
مقیاس توافق	کاپا	۰.۷۸۲	۰.۲۷۱	۲.۴۱۶	۰.۰۴
	تعداد موارد معتبر	۶۳			

با توجه به مفاهیم بدست آمده از مرحله قبل، در این مرحله با انجام بارها مطالعه و بررسی مجدد و فرآیند رفت و برگشت بین مفاهیم و مقولات، با در نظر گرفتن مطالعات مختص به هر مقوله، نتایج مطالعات اصلی و اساسی مر بوط به آن مقوله در کنار هم قرار گرفته و تحلیل شد. عوامل و مولفه‌های تامین امنیت فناوری اطلاعات با رویکرد خطمشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور کدامند؟

مصاحبه با خبرگان (تحلیل مضمون)

برای شناسایی عوامل و مؤلفه‌های تأمین امنیت فناوری اطلاعات با رویکرد خطمشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور، پژوهشی کیفی با روش تحلیل مضمون و با استفاده از نرم‌افزار MAXQDA نسخه ۱۲ انجام شد. جامعه خبرگان این پژوهش را ۱۲ نفر از اساتید دانشگاهی، صاحب‌نظران و پژوهشگران با حداقل مدرک دکتری، دارای تجربه و سابقه کاری مرتبط، اشتغال به تدریس در دانشگاه و سابقه پژوهشی در حوزه امنیت فناوری اطلاعات تشکیل دادند که به صورت هدفمند و با در نظر گرفتن اشباع نظری انتخاب شدند. پس از انجام مصاحبه‌های عمیق با خبرگان و تحلیل پاسخ‌های آنها، (که نمونه‌ای از کدگذاری این مصاحبه هادر جدل شماره ۲ آورده شده است) شبکه مضامین تحقیق با ۶ مضمون فراگیر، ۲۳ مضمون سازمان‌دهنده و ۲۵۳ مضمون پایه شکل گرفت. از روش تحلیل مضمون به عنوان یکی از مهمترین روش‌های تحلیل کیفی استفاده شد که امکان شناخت، تحلیل و گزارش الگوهای موجود در داده‌های کیفی را فراهم می‌کند و داده‌های پراکنده حاصل از مصاحبه‌ها را به داده‌هایی غنی و تفصیلی تبدیل می‌نماید. کدهای استخراج شده از تحلیل مصاحبه‌ها، شاخص‌های اصلی ابعاد و مؤلفه‌ها را تشکیل دادند که هر یک نشان‌دهنده بخشی از عوامل و مؤلفه‌های تأثیرگذار بر تأمین امنیت فناوری اطلاعات با رویکرد اخلاق حرفه‌ای در شهرداری‌های کشور می‌باشند. این پژوهش با هدف ارائه چارچوبی جامع برای مدیریت امنیت فناوری اطلاعات مبتنی بر اصول اخلاق حرفه‌ای در شهرداری‌ها انجام شد و نتایج آن می‌تواند راهنمای مناسبی برای سیاست‌گذاری و برنامه‌ریزی در این حوزه باشد.

هر یک از شرکت‌کنندگان مهمترین ابعاد و مؤلفه‌های تأمین امنیت فن‌آوری اطلاعات مبتنی بر خطمشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور را عنوان کردند. در جدول شماره ۲ نمونه‌ای از کدگذاری‌ها آورده شده است.

جدول ۲. نمونه کدگذاری

کد مشارکت‌کننده	قسمتی از مصاحبه	کدهای استخراج شده
کد: ۲	رعایت نظم در سازمان برای موفقیت یک کسب و کار ضروری است و هر کارفرمایی مایل است تا نظم و انضباط سازمانی را در کسب و کار خود حفظ کند. برای این کار لازم است با کارکنان خود ارتباطی شفاف داشته باشید، با آنها با عزت و احترام رفتار کنید و سعی کنید مسائل و چالش‌های پیش روی آنها را حل کنید. همچنین می‌توانیم از ابزارهای اتوماسیون برای نظم‌دهی و نظارت بر فعالیت‌های کارکنان خود استفاده کنیم. حفظ یک محیط کاری دلپذیر و نظارت مناسب بر رعایت نظم و اجرای قوانین در سازمان، موجب تشویق کارکنان و ایجاد یک نیروی کار شاد، متحد و سازنده خواهد شد. لازم است تمامی کارمندان سازمان دارای هر موقعیت شغلی که باشند، خود را با قوانین و مقررات سازمان وفق دهند. این موضوع از به وجود آمدن هرج و مرج در محیط کار جلوگیری می نماید. رعایت نظم در هر سازمانی سبب به وجود آمدن محیطی سالم برای کسب و کار می گردد. به این صورت دستیابی به اهداف سازمان راحت تر می شود. در ارتباط با دیگران باید به حریم خصوصی دیگران احترام بگذاریم و با کلام و رفتارمان آن مرزبندی‌ها را رد نکنیم. حریم شخصی و خصوصی صرفا به معنای رازهای مگو نیست. این حریم، مرزبندی‌های مختلفی است که هر فرد درحیطه‌های مختلف، دور زندگی‌اش می‌کشد و از دیگران انتظار دارد که به این مرزها تجاوز نکنند. این حریم، بسته به شخصیت، عقیده، قوم، مذهب، نگرش و در نهایت احساسات هر فرد، متفاوت است.	رعایت نظم در سازمان؛ ارتباطی شفاف؛ رفتار با عزت و احترام؛ تشویق کارکنان؛ اجرای عدالت؛ رفتار صادقانه با کارکنان؛ حمایت از شخصیت و کرامت؛ امانتداری؛ اهمیت به درستکاری و خوشنامی در کار؛ خلوص نیت؛ انتقاد از سازمان از سر دلسوزی و خیرخواهی ؛ آمادگی برای پذیرش مسئولیت‌های جدید، توانایی تشخیص اطلاعات مهم از غیر مهم مرتبط با شغل در طی تجزیه و تحلیل مشاغل و پس از آن؛ رقابت شرافتمندانه با دیگر همکاران؛ رعایت انصاف و عدالت، بدون تخریب دیگر همکاران؛ ارتباطات؛ انتقال حس ارزشمندی؛ توسعه؛ حرفه‌ای منابع انسانی؛ صداقت در گفتار و عمل؛ خوش اخلاقی؛ صبر و حوصله؛ ایجاد نظم در کار و حس انجام وظیفه در سازمان؛ طراحی و سازماندهی کتابچه راهنمای اخلاق در محیط کار مخصوص سازمان؛ رعایت و احترام نسبت به ارزشها و هنجارهای اجتماعی

هم اکنون با توجه به چارچوب و مراحل بیان شده جهت ترسیم شبکه مضامین، نتایج حاصل از مصاحبه با شرکت کنندگان مورد تجزیه و تحلیل قرار گرفت و شبکه مضامین تحقیق با ۶ مضمون فراگیر، ۲۳ مضمون سازمان دهنده و ۲۵۳ مضمون پایه شناسایی شد.

جدول ۳. شبکه مضامین ابعاد و مؤلفه‌های مدیریت تأمین امنیت فن‌آوری اطلاعات مبتنی بر خطمشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور

مضامین فراگیر	مضامین سازمان دهنده	مضامین پایه
اخلاق حرفه‌ای	احترام و کرامت	خوشرفتاری
		خوشرویی
		خوشخویی
		احترام متقابل
		تواضع
		صداقت
		رفتار با عزت و احترام
		حمایت از شخصیت و کرامت
		آموزش نسبت به برخوردهای اجتماعی و فرهنگی و خانوادگی
		گنجاندن احترام به کرامت انسانی را در قواعد خود
	انصاف و برابری	دریافت حقوق و پاداش براساس عملکرد
		حقوق عادلانه
		رعایت انصاف و عدالت
		رعایت عدل و انصاف در اجرای سیاست‌های مربوط به حقوق، پاداش و ارتقای آنان
		اجرای عدالت
		رفتار صادقانه با کارکنان

مضامین فراگیر	مضامین سازمان دهنده	مضامین پایه
		رفتار منصفانه
		رعایت عدالت در انجام وظیفه
		پرداخت حق و حقوق پرسنل با رعایت انصاف
		برخورد منصفانه و خیرخواهانه
		خودداری از تبعیض و رفتار توهین آمیز
		عدالت در سازمان‌ها
	رعایت ارزش‌های اجتماعی	حفظ آبروی دیگران
		رعایت حریم شخصی
		رازداری
		امانتداری
		حفظ اسرار اداری
		رعایت حقوق فردی و اجتماعی
	همدردی و همراهی با دیگران	درک کارمندان
		ترجیح منافع جمعی بر شخصی
		انعطاف پذیری مدیر
		پرهیز از خودبینی و خوپسندی
		برآورده ساختن نیازهای کارکنان در محیط کار
		فراهم آوردن تسهیلات و امکانات رفاهی جهت پرسنل سازمان
تعهد و مسئولیت‌پذیری	پاسخگویی	ایجاد الزام در مسئولیت و پاسخگویی مدیران در قبال تصمیمات غلط ایشان
		پاسخگوئی
		پاسخگویی در برابر رفتارها و کارهای انجام شده
	وفاداری	تعهد یا وفاداری سازمانی در محیط کار
		تعهد خویشتن مدارانه
		انتقاد از سازمان از سر دلسوزی و خیرخواهی
		دلبستگی عضو سازمان به سازمان
		آگاهی نسبت به تعهد سازمانی
		تعهد
		بکارگیری افراد امین خداترس و دارای وجدان کار
خلاقیت و نوآوری	سازمانی	حمایت، پشتیبانی و تشویق لازم مدیران
		ساختار سازمانی مناسب
		فضای خلاق
		اعطای اختیار عمل
		تدوین آیین‌نامه‌هایی در جهت حمایت از نظرات کارکنان و تشویق آنها به ارائه نظر در چارچوب استقرار نظام پاداشدهی مناسب برای پیشنهادات خلاق و استفاده از آنها در امور اجرایی
		شکوفاسازی استعداد کارکنان با حمایت از نظرات و اجرای آنها
		آموزش‌های لازم قبل از اجرای خلاقیت و نوآوری
		ایجاد محیطی امن برای بروز افکار کارکنان
		تشویق اعضای تیم به تصمیم گیری درباره چگونگی دستیابی به اهداف
		استقلال کافی کارمندان
		اختصاص زمان لازم برای ارائه افکار خلاق
		برقراری یک سیستم پیشنهادات
		ایجاد واحد مخصوص خلاقیت
		تشویق تجربه کردن
		تغییر فرهنگ سازمانی در راستای سازمان های یادگیرنده
		شناسایی و حذف موانع داخلی

مضامین فراگیر	مضامین سازمان دهنده	مضامین پایه
	فردی	نــگاه مثبــت بــه مشــکلات در جهــت بهبود امــور و ارائــه خدمت مفید
		برنامه‌ریزی مناسب
		آشنایی و داشتن تسلط به حوزه تصدیگری و جایگاه خود
		داشتن اطلاعات صحیح و درست
		اشتیاق و انگیزه بالا در انجام وظایف
مدیریت منابع انسانی	آموزش	تغییر فرهنگ سازمانی در راستای سازمان‌های یادگیرنده
		طراحی و سازماندهی کتابچه راهنمای اخلاق در محیط کار مخصوص سازمان
		تمایل کارکنان به کمک داوطلبانه به یکدیگر
		نگرش مثبت میان مدیران، همکاران و کارکنان نسبت به مشارکت در فعالیت های آموزشی
		برگزاری کارگاههای آموزشی و توجیهی
		پرورش و رشد اخلاق پرسنل و اخلاق مداری در انجام وظایف
		آموزش کارکنان
	توانمندسازی و ارتقاء مهارت	اجرای برنامه هایی با هدف انگیزش
		آموزش مهارتهای هوش هیجانی
		افزایش کارآیی نیروها
		برداشتن گام‌هایی برای بهبود بهره‌وری سازمان شامل ایجاد انگیزه در کارکنان و ارائه بهترین ابزار ممکن برای انجام کارشان
		بهبود دانش، مهارت و توانمندی
		تشویق فعالانه آموزش و توسعه دانش اعضا
		استفاده از فنون فناوری‌های نو توسط سازمان
		رقابت شرافتمندانه با دیگر همکاران
		توسعه حرفه‌ای منابع انسانی
		خودشناسی
		برخورداری کارکنان از آگاهی لازم
		اشتیاق مدیران برای ارائه اطلاعات به فراگیران در این زمینه که، چه طور دانش، مهارت و رفتارهای فراگرفته را در کارشان به طور مؤثر مورد استفاده قرار دهند و چگونه فرصت هایی برای فراگیران ایجاد کنند تا محتوای آموزشی را در کارشان به کار گیرند
		اجرای راه کارهای افزایش کارایی و عملکرد در سازمان
		برگزاری دوره‌ای اموزشی اخلاقی و مذهبی برای پرسنل
		حرکت به سوی رشد و ارتقای کارمندان
		شناسایی ضعف ها و قوت‌های فردی با ارزیابی شایستگی
		پشتکار جِدّی
		خوداتکایی
		داشتن پشتکار و نداشتن هراس از نتیجه کار
	انگیزش	اجرای برنامه هایی با هدف انگیزش
		ایجاد علاقه به کار
		توجه از سوی مدیران و قدرشناسی
		تشویق کارکنان
		پشتیبانی از تعادل بین کار و زندگی و رفاه کارکنان
		تشویق و ایجاد روحیه مثبت در کارکنان
		تقویت ارزش‌های اخلاقی با تشویق و قدردانی و دادن پاداش به کارکنان متعهد و مسئولیت پذیر
		ایجاد انگیزه به روش‌های مختص برای هر فرد
		طراحی نظام ارزیابی عملکرد براساس عملکرد – پاداش
		روحیه کارمندان
		پشتیبانی از تعادل بین کار و زندگی و رفاه کارکنان

مضامین فراگیر	مضامین سازمان دهنده	مضامین پایه
		انگیزش کارکنان
		استفاده از شیوه‌های رهبری مؤثر
		استفاده از شیوه‌های پرداخت تشویقی
	جبران خدمات	انتقال حس ارزشمندی
		دریافت احساس ارزشمندی از طرف سازمان
		ارزشمند شمردن کارکنان و قدردانی از آن ها
		پاداش به موفقیت ها و به شکست ها به فراخور
	مشارکت	استفاده از برنامه های مدیریت مشارکتی
		مشارکت کارکنان
		انجام کارها به صورت تیمی و با مشارکت همه کارکنان
		وجود زمینه‌های مساعد و فراهم بودن پیش نیازهای مشارکت و شیوه اجرای درست آن
		فعالیت به صورت گروهی و تیمی
		تشویق برای برقراری ارتباطات غیررسمی برای تکمیل و بهبود روابط رسمی
		ایجاد برنامه‌های مشارکتی
		اتحاد و همکاری بین اعضای سازمان
		فراهم ساختن محیطی برای کار تیمی و همفکری و همدلی اعضای سازمان
		برقراری ارتباط بیشتر با هم تیمی ها
		زمینه‌سازی و بسترسازی در بین کارکنان جهت ایجاد فرهنگی که در آن همگان در تلاش برای رشد دادن دیگری هستند و با تأثیر بر روی یکدیگر به پیشرفت مجموعه و سازمان کمک کنند
		تسهیم اطلاعات بین کارکنان
		داشتن روحیهٔ همکاری و اهداف مشترک
	مدیریت عملکرد	برنامه‌ریزی
		نظارت
		توسعه
		رتبه‌بندی و پاداش
عمکرد منابع انسانی	تصمیم گیری	انعطاف پذیری در تصمیم گیری
		مهارت‌های تصمیم گیری
		تصمیم گیری بر اساس اصول علمی
		تعهد و پایبندی نسبت به تصمیمات و برنامه
		تصمیم گیری اخلاقی
	رفتار فردی	رفتار
		خویشتنداری، شکیبایی و خودداری از شکایت در ناگواریها و سختیها
		فرهنگ
		ظرفیت پذیرش رویدادهای گوناگون
		خستگی ناپذیری
		خوش قولی
		خلوص نیت
		خوش اخلاقی
		صبر و حوصله
		پرهیز از حسد
		هدفمنـــد بودن در زندگی
		اخلاق پسندیده
		داشتن صبر و شکیبایی
		تکامل
		تخصص

مضامین فراگیر	مضامین سازمان دهنده	مضامین پایه
		نفوذ کلام
		تهذیب نفس
		پرهیز از شتابزدگی
		پرهیز از شتابزدگی و عجله
		تسلیم ناپذیری در بحران‌ها
	رفتار سازمانی	رضایت شغلی
		وقت شناسی (مدیریت زمان)
		آمادگی برای پذیرش مسئولیت‌های جدید
		توانایی تشخیص اطلاعات مهم از غیر مهم مرتبط با شغل در طی تجزیه و تحلیل مشاغل و پس از آن
		رعایت و احترام نسبت به ارزشها و هنجارهای اجتماعی
		سازگاری با اهداف سازمانی
		برخورداری مدیران و کارمندان از توانمندی‌های روحی و روانی
		توانایی مواجه با مشکلات و ایده‌های مخالف
		پشتیبانی اجتماعی
		پذیریش مسؤولیت رفتار یا عملکرد
		داشتن روابط عمومی
		شـــناخت از محیـــط کار
		درک دقیق مشکل و یا خواسته مشتری و ارائه راه حل مناسب
		شناسایی نقاط قوت و ضعف با ارزیابی شایسته افراد در سازمان
		رواج اخلاق هنجاری که قابل قبول در اداره
		درک بر مسئولیت پذیری و تعهد
		قرار گرفتن براساس شایسته گی و تخصص وتحصیلات وآموزش درست در هر پست و جایگاهی
		بهره مندی از اطلاعات درست در مورد همه چیز
		مسئولیت پذیری در قبال رفتار
		شناخت مناسب از نحوه تاثیرگذاری اعتماد و صداقت رفتاری
		ادراک سیاست‌های سازمانی
		پذیرش انتقاد
		وجدان کاری و انضباط اجتماعی
		رعایت اصول آداب معاشرت در محیط کار
		یاری رساندن به همکاران
		امانتداری از کار و مسئولیت
		خدمت به خلق
		احساس مسئوولیت
		اخلاق و رفتار حرفه‌ای
ساختار سازمان	رسمیت	یکپارچه نمودن نیازهای سازمان با نیازهای فردی اعضای آن
		استاندارد کردن فعالیت‌های سازمانی
		صحت و دقت اطلاعات و کنترل صحت، دقت و پویایی آن
		ایجاد انسجام و پویایی در سازمان با حداقل کنترل و نظارت غیر مستقیم مدیر
		بهینه سازی تعداد کارکنان
		قرار دادن مبنای پاداش ها و مجازات ها بر اصل شایسته سالاری
	پیچیدگی	عدم تمرکزگرایی سازمانی و کاهش هزینه ها
		اتوماسیون و کاهش عملیات دستی
		افزایش سرعت و سادگی کار
		سیستم های یکپارچه اطلاعات مدیریت (MIS) با هدف استفاده بهینه از فناوری ارتباطات و اطلاعات
		توجه به جزئیات موجود در فرآیند استخدام، ارزیابی عملکرد و...

مضامین فراگیر	مضامین سازمان دهنده	مضامین پایه
	حفاظت و پشتیبانی	مدیریت از راه دور
		امنیت اطلاعات
		حفاظت از سرورها
		خدمات پشتیبانی اختصاصی
		ایمنی سامانه از اشتباهات عمدی
		طرّاحی فرایند خطاناپذیری کار
	عملکرد سازمان	شاخص‌ها و اهداف سازمانی
		بکارگیری افراد با استعداد و ایمان کاری ودریافت اطلاعات انها در تصمیمات با در نظر گرفتن جنبه‌های مادی و معنوی
		مدل‌های مناسب تشویق و تنبیه
		نظام تشویق و تنبیه
		چگونگی رقابت بین اعضای سازمان
		راهکارهای سازمانی
		کنترل جابه‌جایی افراد
		کنترل سرمایه
		برقراری ارتباط بین کارها و منابع تمام بخش‌های مختلف یک سازمان، به‌منظور رسیدن به هدف مشخص و مشترک
		سبک رهبری
		استراتژی
		عملکرد و معیارها
		برآورده ساختن نیازهای کارکنان در محیط کار
		شفافیت
		عمل کردن به وعده‌های داده شده و تعهدات
		یکسان بودن ادعا و عمل
		حقایق را درست جلوه دادن
		عدم جمود فکری
		بهبود جو سازمانی
	ارتباطات و تعامل	یگانگی نسبی اهداف اعضاء و ســازمان
		انعطاف پذیری مدیر
		ارتباطی شفاف
		ارتباطات
		رقابت سالم شرکت‌ها
		ارتباط مدیر با پرسنل، هم صنف‌ها و زیر دستان
		یاری رساندن به دیگران
		فراهم آوردن تسهیلات و امکانات رفاهی جهت پرسنل سازمان
		برخورد قانونی و موثر با پرسنل
		اخلاق مناسب مدیران جهت اخذ اطلا عات از پرسنل
		اولویت‌های انتخاب مدیر براساس میزان ادب و صداقت و تخصص فرد
		الگو بودن برای کارکنان
		برقراری ارتباط چشمی
		همدردی با کارمندان
		برخورد قاطعانه در صورت لزوم
		اعتماد کارکنان به مدیرشان
		رفتاری صادقانه و شفاف با همکاران و پرهیز از ریاکاری
		احترام به افکار دیگران
	مدیریت اطلاعات	یکپارچه سازی اطلاعات

مضامین فراگیر	مضامین سازمان دهنده	مضامین پایه
		سامانهٔ کنترل منشأ پیدایش اطلاعات
		دریافت اطلاعات درست
		دریافت بموقع اطلاعات
		جلوگیری از ضایع شدن اطلاعات
		ذخیره و پشتیبان‌گیری
		عدم جلوگیری از تبادل اطلاعات (حبس اطلاعات)
	رعایت نظم و مقررات	ایجاد نظم در کار و حس انجام وظیفه در سازمان
		قانونمندی
		استفاده از ابزار ها ی کنترلی در رعایت نظم و انظباط اداری
		اولویت بندی وظایف
		یک‌پارچگی اطلاعات واحدها
		هماهنگی پردازش اطلاعات
		انجام به موقع کارها
		سازگاری با قوانین و مقررات سازمان

یافته‌های حاصل از جدول شماره ۲ که با هدف شناسایی عوامل و مؤلفه‌های تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور انجام شده است، حاصل تحلیل محتوای مصاحبه‌های عمیق با ۱۲ نفر از خبرگان این حوزه می‌باشد. نتایج تحلیل‌ها منجر به شناسایی ۶ مضمون فراگیر، ۲۴ مضمون سازمان‌دهنده و ۲۵۳ مضمون پایه گردید که چارچوب جامعی برای تأمین امنیت فناوری اطلاعات در شهرداری‌ها ارائه می‌دهد.

در این میان، مضمون فراگیر "ساختار سازمان" با ۸۳ کد و هفت مضمون سازمان‌دهنده بیشترین فراوانی را به خود اختصاص داده است. این امر نشان می‌دهد که در شهرداری‌های کشور، توجه به ساختارهای سازمانی مناسب، رعایت نظم و مقررات، مدیریت صحیح اطلاعات و برقراری ارتباطات و تعاملات سازنده، نقش کلیدی در تأمین امنیت فناوری اطلاعات دارد. به‌ویژه، یکپارچه‌سازی اطلاعات، استانداردسازی فعالیت‌ها و ایجاد سیستم‌های یکپارچه اطلاعات مدیریت (MIS) از اهمیت ویژه‌ای برخوردار است.

"مدیریت منابع انسانی" با ۶۴ کد و شش مضمون سازمان‌دهنده در رتبه دوم قرار دارد که نشان‌دهنده اهمیت سرمایه انسانی در تأمین امنیت فناوری اطلاعات است. در شهرداری‌ها، توجه به آموزش مستمر کارکنان، توانمندسازی و ارتقای مهارت‌های آنها، ایجاد انگیزه و مشارکت در تصمیم‌گیری‌ها از عوامل کلیدی محسوب می‌شود. به‌ویژه، برگزاری دوره‌های آموزشی تخصصی در حوزه امنیت فناوری اطلاعات و اخلاق حرفه‌ای، طراحی نظام انگیزشی مناسب و ایجاد فرصت‌های مشارکت برای کارکنان از اهمیت بالایی برخوردار است.

مضمون "عملکرد منابع انسانی" با ۶۲ کد و سه مضمون سازمان‌دهنده بر اهمیت رفتارهای فردی و سازمانی کارکنان تأکید دارد. در شهرداری‌ها، تصمیم‌گیری‌های اخلاقی، رفتارهای حرفه‌ای، وجدان کاری و انضباط اجتماعی نقش مهمی در تأمین امنیت فناوری اطلاعات ایفا می‌کنند. همچنین، رضایت شغلی، سازگاری با اهداف سازمانی و توانایی مواجهه با مشکلات از عوامل تأثیرگذار در این حوزه هستند.

"اخلاق حرفه‌ای" با ۵۰ کد و چهار مضمون سازمان‌دهنده بر ضرورت رعایت اصول اخلاقی در محیط کار تأکید دارد. در شهرداری‌ها، احترام به کرامت انسانی، رعایت انصاف و عدالت، حفظ ارزش‌های اجتماعی و همدردی با دیگران از عوامل کلیدی در تأمین امنیت فناوری اطلاعات محسوب می‌شوند. به‌ویژه، رازداری، امانتداری و حفظ اسرار اداری از اهمیت ویژه‌ای برخوردار است.

مضامین "خلاقیت و نوآوری" با ۲۳ کد و "تعهد و مسئولیت‌پذیری" با ۱۱ کد نیز بر اهمیت نوآوری سازمانی و فردی و همچنین پاسخگویی و وفاداری سازمانی تأکید دارند. در شهرداری‌ها، ایجاد فضای خلاق، حمایت از نوآوری، تعهد سازمانی و مسئولیت‌پذیری از عوامل مؤثر در تأمین امنیت فناوری اطلاعات هستند.

این یافته‌ها نشان می‌دهد که تأمین امنیت فناوری اطلاعات در شهرداری‌های کشور، علاوه بر جنبه‌های فنی و زیرساختی، نیازمند توجه ویژه به ابعاد انسانی، اخلاقی و رفتاری است. همچنین، ضرورت ایجاد ساختارهای سازمانی مناسب، توانمندسازی کارکنان و ترویج فرهنگ اخلاق حرفه‌ای در این سازمان‌ها مشهود است. این ابعاد و مؤلفه ها می‌تواند به عنوان چارچوبی جامع برای برنامه‌ریزی و اجرای اقدامات مرتبط با تأمین امنیت فناوری اطلاعات در شهرداری‌های کشور مورد استفاده قرار گیرد.

نتیجه‌گیری

در عصر حاضر که فناوری اطلاعات نقشی محوری در تمامی عرصه‌های مدیریت شهری ایفا می‌کند، مسئله تأمین امنیت داده‌ها و اطلاعات به یکی از چالش‌های اساسی شهرداری‌ها تبدیل شده است. شهرداری‌ها به عنوان نهادهای عمومی غیردولتی، روزانه با حجم عظیمی از اطلاعات شخصی شهروندان، داده‌های مالی، اسناد حقوقی و مستندات شهرسازی سروکار دارند که حفاظت از آنها در برابر تهدیدات سایبری و سوءاستفاده‌های احتمالی، امری حیاتی به شمار می‌رود. در این میان، نقش عامل انسانی و به طور خاص، رعایت اصول اخلاق حرفه‌ای توسط کارکنان، اهمیتی دوچندان می‌یابد. پژوهش حاضر با هدف شناسایی عوامل و مولفه‌های تامین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور انجام شده است. یافته‌های این مطالعه نشان می‌دهد که موفقیت در تأمین امنیت اطلاعات، مستلزم توجه همزمان به سه بعد زمینه‌ای، رفتاری و ساختاری است. در بعد زمینه‌ای، عواملی همچون احترام به حریم خصوصی شهروندان، رعایت انصاف و برابری در دسترسی به اطلاعات، پایبندی به ارزش‌های اجتماعی و همدلی با ذینفعان مورد توجه قرار می‌گیرد. بعد رفتاری به مؤلفه‌هایی چون مدیریت عملکرد، تصمیم‌گیری‌های اخلاقی، رفتار سازمانی و رفتار فردی می‌پردازد که نقشی کلیدی در حفظ امنیت اطلاعات ایفا می‌کنند. در بعد ساختاری نیز، عناصری مانند طراحی ساختار سازمانی منعطف و پاسخگو، تدوین قوانین و مقررات شفاف و کارآمد، و ایجاد زیرساخت‌های فنی مناسب مورد بررسی قرار می‌گیرند. نتایج پژوهش‌های مشابه در این حوزه نیز تأیید می‌کند که سازمان‌هایی که توانسته‌اند اصول اخلاق حرفه‌ای را در فرهنگ سازمانی خود نهادینه کنند، عملکرد بهتری در مقابله با تهدیدات امنیتی داشته‌اند. به عنوان نمونه، مطالعات نشان می‌دهد که آموزش‌های مستمر در زمینه اخلاق حرفه‌ای می‌تواند تا ۶۰ درصد ریسک‌های امنیتی را کاهش دهد. همچنین، سازمان‌هایی که دارای منشور اخلاقی مشخص در حوزه امنیت اطلاعات هستند، موفقیت بیشتری در پیشگیری از حوادث امنیتی داشته‌اند. این پژوهش تأکید می‌کند که برای دستیابی به سطح مطلوبی از امنیت فناوری اطلاعات در شهرداری‌ها، باید رویکردی جامع و یکپارچه اتخاذ شود که در آن، علاوه بر جنبه‌های فنی و تکنولوژیک، به ابعاد انسانی و اخلاقی نیز توجه ویژه‌ای شود. در این راستا، پیشنهاد می‌شود شهرداری‌ها با تدوین خط‌مشی‌های اخلاقی شفاف، برگزاری دوره‌های آموزشی منظم، ایجاد سیستم‌های تشویقی برای رفتارهای امنیتی مطلوب، و پایش مستمر عملکرد کارکنان، زمینه را برای ارتقای سطح امنیت اطلاعات فراهم آورند. همچنین، ضروری است که این خط‌مشی‌ها به طور مستمر مورد بازنگری و به‌روزرسانی قرار گیرند تا با تحولات سریع فناوری و تهدیدات نوظهور همگام باشند. این پژوهش با شناسایی ۲۲ مؤلفه و ۲۲۵ شاخص در قالب سه بعد اصلی، چارچوبی جامع برای مدیریت امنیت فناوری اطلاعات در شهرداری‌ها ارائه می‌دهد که می‌تواند راهنمای عمل مدیران و کارشناسان در این حوزه باشد.

نتایج این پژوهش با یافته‌های محققانی همچون سلحشوری و همکاران (۱۴۰۱)، طاهری‌راد و ویسی (۱۴۰۱)، حمیدی (۱۴۰۰)، خلیفه و همکاران (۱۴۰۰)، کلانتری و دیگران (۱۳۹۹)، اخوان و رادفر (۱۳۹۹)، حدادی هرندی و دیگران (۱۳۹۸)، هادی و همکاران (۲۰۲۴)، ناودیپ و همکاران (۲۰۲۳)، هیلهورست[1] و همکاران (۲۰۲۲)، القمدی[2] و همکاران (۲۰۲۲)، کارال[3] (۲۰۲۱)، منبارو (۲۰۲۱)، همسو است که همگی بر نقش محوری اخلاق حرفه‌ای در موفقیت برنامه‌های امنیت اطلاعات تأکید کرده‌اند. این پژوهشگران نشان داده‌اند که رعایت اصول اخلاقی توسط کارکنان، نه تنها به کاهش چشمگیر حوادث امنیتی منجر می‌شود، بلکه می‌تواند به عنوان یک مزیت رقابتی برای سازمان‌ها در عصر دیجیتال عمل کند. در مجموع، این پژوهش با ارائه رویکردی نوین

1 Hilhorst
2 AlGhamdi
3 Karale

به مقوله امنیت فناوری اطلاعات که در آن اخلاق حرفه‌ای به عنوان عنصری کلیدی مورد توجه قرار گرفته است، می‌تواند راهگشای شهرداری‌ها و سایر سازمان‌های عمومی در مواجهه با چالش‌های امنیتی عصر حاضر باشد.

همسویی نتایج پژوهش حاضر با مطالعات پیشین، بیانگر اهمیت و ضرورت توجه به اخلاق حرفه‌ای در مدیریت امنیت فناوری اطلاعات است. همان‌گونه که مشاهده شد، نتایج این پژوهش با یافته‌های محققانی همچون سلحشوری و همکاران (۱۴۰۱)، طاهری‌راد و ویسی (۱۴۰۱)، حمیدی (۱۴۰۰)، خلیفه و همکاران (۱۴۰۰)، کلانتری و دیگران (۱۳۹۹)، اخوان و رادفر (۱۳۹۹)، حدادی هرندی و دیگران (۱۳۹۸)، هادی و همکاران (۲۰۲۴)، ناودیپ و همکاران (۲۰۲۳)، هیلهورست[1] و همکاران (۲۰۲۲)، القمدی[2] و همکاران (۲۰۲۲)، کارال[3] (۲۰۲۱)، منبارو (۲۰۲۱)، همخوانی دارد. این همسویی از آن جهت قابل توجه است که تمامی این پژوهش‌ها، علی‌رغم تفاوت در جامعه آماری و روش‌شناسی، به نتایج مشابهی در خصوص نقش محوری اخلاق حرفه‌ای در تأمین امنیت اطلاعات دست یافته‌اند. دلیل این همگرایی را می‌توان در ماهیت انسان‌محور مقوله امنیت اطلاعات جستجو کرد. در واقع، اگرچه جنبه‌های فنی و تکنولوژیک در تأمین امنیت اطلاعات نقشی انکارناپذیر دارند، اما تجربه نشان داده است که بدون توجه به عامل انسانی و به طور خاص، رعایت اصول اخلاق حرفه‌ای توسط کارکنان، حتی پیشرفته‌ترین سیستم‌های امنیتی نیز نمی‌توانند کارایی لازم را داشته باشند. این موضوع در سازمان‌های عمومی همچون شهرداری‌ها که روزانه با حجم عظیمی از اطلاعات حساس شهروندان سروکار دارند، اهمیتی دوچندان می‌یابد. یافته‌های پژوهش‌های مذکور نشان می‌دهد که سازمان‌هایی که توانسته‌اند اصول اخلاق حرفه‌ای را در فرهنگ سازمانی خود نهادینه کنند، نه تنها در پیشگیری از حوادث امنیتی موفق‌تر بوده‌اند، بلکه در صورت بروز مشکلات امنیتی نیز، توانایی بیشتری در مدیریت و کنترل آسیب‌ها داشته‌اند. این مسئله نشان می‌دهد که رویکرد اخلاق‌محور در مدیریت امنیت اطلاعات، فراتر از یک الزام سازمانی، به یک مزیت رقابتی تبدیل شده است. همچنین، همسویی نتایج در خصوص تأثیر آموزش‌های اخلاق حرفه‌ای بر کاهش ریسک‌های امنیتی، اهمیت سرمایه‌گذاری در این حوزه را آشکار می‌سازد. به طور خاص، مطالعات نشان می‌دهند که سازمان‌هایی که برنامه‌های آموزشی منظم در زمینه اخلاق حرفه‌ای برگزار می‌کنند، تا ۶۰ درصد کاهش در حوادث امنیتی را تجربه کرده‌اند. علاوه بر این، همسویی نتایج در خصوص اهمیت ساختار سازمانی منعطف و پاسخگو، ضرورت بازنگری در ساختارهای سنتی و حرکت به سمت مدل‌های چابک‌تر را نشان می‌دهد. این یافته‌ها در مجموع، تأییدی بر رویکرد سه‌بعدی (زمینه‌ای، رفتاری و ساختاری) پژوهش حاضر است که تلاش کرده است با نگاهی جامع و یکپارچه، تمامی جنبه‌های مؤثر بر امنیت اطلاعات را مورد توجه قرار دهد. در نهایت، این همسویی نتایج نشان می‌دهد که موفقیت در تأمین امنیت فناوری اطلاعات، مستلزم اتخاذ رویکردی جامع است که در آن، اخلاق حرفه‌ای به عنوان عنصری محوری و زیربنایی مورد توجه قرار گیرد. این امر به ویژه در شهرداری‌ها که نقشی حیاتی در ارائه خدمات به شهروندان دارند، از اهمیت بسزایی برخوردار است و می‌تواند به عنوان راهنمای عمل مدیران و کارشناسان در طراحی و پیاده‌سازی سیستم‌های امنیت اطلاعات مورد استفاده قرار گیرد.

راستای ارتقای سطح امنیت فناوری اطلاعات در شهرداری‌ها و با توجه به یافته‌های این پژوهش، پیشنهادات کاربردی زیر ارائه می‌گردد. نخست، پیشنهاد می‌شود شهرداری‌ها نسبت به تدوین و استقرار نظام جامع مدیریت امنیت اطلاعات مبتنی بر اخلاق حرفه‌ای اقدام نمایند. این نظام باید دربرگیرنده مجموعه‌ای منسجم از خط‌مشی‌ها، دستورالعمل‌ها و رویه‌های اجرایی باشد که با شرایط و نیازهای خاص هر شهرداری تطبیق یافته است. در این راستا، ایجاد واحد تخصصی امنیت اطلاعات با شرح وظایف مشخص و اختیارات کافی می‌تواند به عنوان گام نخست مورد توجه قرار گیرد. همچنین، برگزاری دوره‌های آموزشی مستمر و هدفمند برای تمامی سطوح سازمانی، از مدیران ارشد تا کارکنان عملیاتی، با تمرکز بر جنبه‌های اخلاقی امنیت اطلاعات ضروری است. این آموزش‌ها باید به گونه‌ای طراحی شوند که علاوه بر انتقال دانش فنی، به تقویت حس مسئولیت‌پذیری و تعهد اخلاقی کارکنان نیز منجر شوند. علاوه بر این، پیشنهاد می‌شود سیستم ارزیابی عملکرد کارکنان به گونه‌ای بازطراحی شود که رعایت اصول اخلاقی در حوزه امنیت اطلاعات به عنوان یکی از شاخص‌های کلیدی عملکرد در نظر گرفته شود. در این راستا، طراحی و

1 Hilhorst
2 AlGhamdi
3 Karale

اجرای نظام جامع پاداش و تنبیه مبتنی بر عملکرد امنیتی کارکنان می‌تواند به تقویت انگیزه‌های درونی و بیرونی برای رعایت اصول اخلاقی کمک کند. همچنین، ایجاد کانال‌های ارتباطی مؤثر برای گزارش‌دهی حوادث امنیتی و حمایت از کارکنانی که تخلفات امنیتی را گزارش می‌کنند، می‌تواند به تقویت فرهنگ شفافیت و پاسخگویی در سازمان کمک نماید. از سوی دیگر، پیشنهاد می‌شود شهرداری‌ها نسبت به توسعه زیرساخت‌های فنی خود متناسب با آخرین استانداردهای امنیتی اقدام نمایند و سیستم‌های نظارتی هوشمند برای شناسایی و پیشگیری از تخلفات امنیتی را مستقر سازند. در نهایت، برقراری ارتباط مؤثر با ذینفعان خارجی، به ویژه شهروندان، و آگاه‌سازی آنها نسبت به اهمیت حفظ امنیت اطلاعات می‌تواند به ایجاد یک اکوسیستم امن و قابل اعتماد کمک کند. این پیشنهادات باید در قالب یک برنامه اقدام مشخص با اولویت‌بندی زمانی و تخصیص منابع کافی به اجرا درآیند و به طور مستمر مورد پایش و ارزیابی قرار گیرند تا اثربخشی آنها تضمین گردد. علاوه بر این، پیشنهاد می‌شود شهرداری‌ها با ایجاد کارگروه‌های تخصصی متشکل از متخصصان فناوری اطلاعات، کارشناسان امنیت و متخصصان اخلاق حرفه‌ای، به طور مستمر نسبت به بازنگری و به‌روزرسانی خط‌مشی‌های امنیتی خود اقدام نمایند تا بتوانند با تهدیدات نوظهور در فضای سایبری مقابله کنند.

منابع

۱. اخوان، فاطمه و رادفر، رضا. (۱۳۹۹). ارائه مدلی برای پایش بلوغ امنیت اطلاعات. فصلنامه رشد فناوری، ۱۶(۶۴): ۱۰-۱.

۲. حدادی هرندی، علی اکبر؛ والمحمدی، چنگیز و صالحی صدیقیانی، جمشید. (۱۳۹۸). مدیریت امنیت اطلاعات در سازمان هوشمند، دوفصلنامه علمی و پژوهشی مدیریت بحران، ویژه نامه هوشمندسازی، ۳۳ (۲۵): ۱۵-۱.

۳. حمیدی آشتیانی، سامان. (۱۴۰۰). بررسی عناصر راهبردی فناوری اطلاعات و همراستایی آن با امنیت اطلاعات تجارت سازمانی. چهارمین همایش ملی و نخستین همایش بین‌المللی الگوهای نوین مدیریت و سازمان، تهران.

٤. خلیفه سلطانی، حشمت؛ تشکری بهشتی، پریسا و چینی چیان مقدم، ایمان. (۱۴۰۰). بحران اخلاق زدایی و گسترش اخلاق در متخصصین فناوری اطلاعات. هجدهمین همایش بین‌المللی مدیریت، تهران.

۵. دوستی، مهدی. (۱۴۰۲). اخلاق حرفه ای در فناوری اطلاعات. دو ماهنامه مهندسی مدیریت، ۱۶(۸۵)، ۳۷.

٦. ده دست، ناصر. (۱۴۰۰). بررسی و شناسایی مؤلفه های اخلاق حرفه ای (مطالعه موردی شهرداری تهران). ماهنامه آفاق علوم انسانی، ۵(۵۶)، ۱-۱۷.

۷. سلحشوری، فرهاد؛ ریگی، محسن و کیخا، سمیه. (۱۴۰۱). بررسی و تبیین امنیت داده‌ها. دومین همایش بین‌المللی مهندسی برق، رایانه و مکانیک.

۸. سهرابی، شهلا؛ شمس، حسین و عزیزی نژاد، حسین. (۱۴۰۰). نقش اخلاق حرفه‌ای اسلامی در موفقیت سازمان‌های پروژه محور ایران. فصلنامه پژوهش‌های علوم مدیریت، ۳(۷): ۱۵-۱.

۹. شاکری، محمد جواد؛ مخترع، آیدا و رستگاری، بهنام. (۱۴۰۴). کاربرد فناوری زنجیره‌های بلوکی در تأمین امنیت اطلاعات الکترونیک قضایی. فصلنامه مطالعات میان رشته‌ای فقه، ۵(۲)، ۱۷-۱.

۱۰. طاهری‌راد، زهرا و ویسی، پرهام. (۱۴۰۱). پیاده‌سازی مرکز عملیات امنیت SOC در سازمان فناوری اطلاعات و ارتباطات شهرداری شیراز. پانزدهمین همایش بین‌المللی فناوری اطلاعات، رایانه و مخابرات.

۱۱. عیدی، فاطمه؛ کردی، مراد و علیزاده جورکویه، ابراهیم. (۱۴۰۲). ارتقاء عملکرد بانکداری الکترونیک از طریق توجه به قابلیت های فناوری اطلاعات، شیوه های مدیریت زنجیره تامین و مدیریت ریسک امنیت اطلاعات. نشریه مطالعات نوین بانکی، ۶(۱۸): ۸-۴۰.

۱۲. غمخواری، سیده معصومه؛ نبی نیا، علیرضا و رسولی، امیر. (۱۴۰۳). رابطهٔ تعهد سازمانی با رفتار شهروندی سازمانی : نقش میانجی اخلاق حرفه ای. اخلاق در علوم و فناوری، ۱۵۰-۱۴۴.

۱۳. فرامرز پور، فاطمه و فرامرز پور، مهدی. (۱۴۰۲). بررسی تاثیر فرهنگ سازمانی بر مسولیت اجتماعی و تعهد سازمانی با نقش میانجی اخلاق حرفه ای و رفتار رهبری استراتژیک ، مطالعه موردی کارکنان شهرداری نیشابور. هشتمین کنفرانس بین المللی مطالعات بین رشته ای در مدیریت و مهندسی، دانشگاه تهران.

۱۴. کلانتری، رضا؛ معینی، علی؛ صفری، حسین و عرب سرخی، ابوذر. (۱۳۹۹). ارائه چارچوب مفهومی، برای سنجش عملکرد زنجیره تأمین خدمات امنیت اطلاعات مبتنی بر رویکرد فراترکیب و روش دلفی فازی. مجله مدیریت صنعتی دانشگاه تهران، ۱۲(۱): ۴۶- ۲۴.

۱۵. محمدی، رضا و بسطامی، همت الله. (۲۰۲۴). مدلیابی رابطه علّی بین فضیلت سازمانی و اخلاق حرفه‌ای کارکنان اداره کل ورزش و جوانان استان کرمانشاه با نقش میانجی‌گری مدیریت راهبردی منابع انسانی .*مطالعات مدیریت رفتار سازمانی در ورزش.*

۱۶. محمودی جبدرق، یعقوب؛ پاک مرام، عسگر؛ عبدی، رسول و رضایی، نادر. (۱۴۰۱). ارائه مدلی برای مدیریت تضاد و تعارض در محیط حسابداری با تاکید بر مولفه های اخلاق حرفه ای. فصلنامه اخلاق در علوم و فناوری، ۱۷(۱)، ۸۹-۷۸.

۱۷. مقیمی خراسانی، علیه. (۱۴۰۲). رابطه سبک رهبری مدیران و اخلاق حرفه‌ای کارکنان. اخلاق در علوم و فناوری، ۱۸(۴)، ۱۹۲-۱۹۶.

۱۸. وظیفه، زهرا؛ مهدی، محمد و وکیلی، نادیا. (۱۳۹۷). الگوی امکان سنجی و استقرار اثربخش سیستم مدیریت امنیت اطلاعات بر مبنای روش فراترکیب. مطالعات مدیریت کسبوکار هوشمند، ۷(۲۶)، ۷۱-۹۹.

19. Akinsanya, M. O., Ekechi, C. C. and Okeke, C. D. (2024). Virtual private networks (vpn): a conceptual review of security protocols and their application in modern networks. Engineering Science & Technology Journal, 5(4), 1452-1472.

20. AlGhamdi, S, et al. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. Government Information Quarterly16 June 2022.

21. Chua, H.N., Ooi, J.S. and Herbland, A. (2021). The effects of different personal data categories on information privacy concern and disclosure. Computers & Security, 110, 102453.

22. De Zoysa, A.H.N. (2022). Inculcating Professional Ethics among Employees in the Workplace A Systematic Literature Review, International Journal of Multidisciplinary Studies (IJMS), Volume 9, Issue I.

23. Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S. and Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: a review. Sensors, 23(3), 1151.

24. Farayola, O. A., Olorunfemi, O. L. and Shoetan, P. O. (2024). Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal, 5(3), 606-615.

25. Hadi, A., Miftachul, H., Novel, L. and Badlihisham, M. N. (2024). 2. Managing Professional-Ethical Negotiation for Cyber Conflict Prevention. International journal of cyber behavior, psychology, and learning, doi: 10.4018/ijcbpl.344022

26. Hakim, A. and Supriyatno, B. (2023). The Effect of Work Ethics and Employee Empowerment on Organizational Performance in Tebet District, South Jakarta Administrative City. International Journal of Education, Business and Economics Research (IJEBER), 3(4), 207-221

27. Hilhorst, C., et al. (2022). Efficiency gains in public service delivery through information technology in municipalities. Government Information Quarterly16 June 2022.

28. Jha, J. and Singh, M. (2023). Who cares about ethical practices at workplace? A taxonomy of employees' unethical conduct from top management perspective. International Journal of Organizational Analysis, 31(2), 317-339
29. Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet of Things16 June 2021.
30. Menbarrow Z. (2021). The Importance and Necessity of Professional Ethics in the Organization and the Role of Managers. Psychology and Behavioral Science International Journal, Volume 18, Issue 1, DOI: 10.19080/PBSIJ.2021.18.555979.
31. Navdeep., Akshay, G., Muskan., Vaibhav, and Sharma. (2023). The Role of Ethics in Developing Secure Cyber-Security Policies. doi: 10.52783/tjjpt.v43.i4.2346
32. Ning, Y. (2022). Information security challenge of modern society. Vestnik Ûžno-Ural′skogo gosudarstvennogo universiteta, 14(2), 65-70, https://www.doi.org/10.14529/ped220206.
33. Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299-1323.
34. Rao, P. S., Krishna, T. G. and Muramalla, V. S. S. R. (2023). Next-gen cybersecurity for securing towards navigating the future guardians of the digital realm. International Journal of Progressive Research in Engineering Management and Science (IJPREMS) Vol, 3, 178-190.
35. Saha, P. (2018). Government e-service delivery: identification of success factors from citizens' perspective (Doctoral dissertation, Luleå tekniska universitet).
36. Saraswat, A. K. and Meel, V. (2022). Protecting data in the 21st century: Challenges, strategies and future prospects. Information technology in industry, 10(2), 26-35
37. Sarwari, A. Sh. and ul Haq, A., (2023). International professional ethics. The Islamic Culture" As-Saqafat-ul Islamia" Research Journal-Sheikh Zayed Islamic Centre, University of Karachi, 48(2), 17-33, http://theislamicculture.com/index.php/tis/article/view/933.
38. Siewert, W. and Udani, A. (2016). Missouri municipal ethics survey: Do ethics measures work at the municipal level? Public Integrity, 18(3), 269-289.
39. Steen, M. E. (2023). Ethics as a Participatory and Iterative Process. Communications of the ACM, 66(5), 27-29, https://www.doi.org/10.1145/3550069.
40. Stergiou, C., Psannis, K. E., Kim, B. G. and Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.
41. Yazdanmehr, A., Li, Y. and Wang, L. (2023). Employee responses to information security related stress: Coping and violation intention. Information Systems Journal, 33(3), 598-639, https://doi.org/10.1111/isj.12417.