ISSN:2821-1588 | htpps://www.jadm.khadu.ir

**Journal of Air Defense Management**
Volume 2, Issue 7
Fall 2023
P.P. 193-214

**Research Paper**

# The Management Model of Information Technology Security Based on Professional Ethics Policies of Employees

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

1. PHD Student of Information Technology Management, Department of Management, Hamedan Branch, Islamic Azad University, Hamedan, Iran. **E-mail: Mostafa.esfandyar@gmail.com**
2. Associate Prof., Computer Department, Hamedan Branch, Islamic Azad University, Hamedan, Iran. **E-mail: Esmaeilpour@iauh.ac.ir**
3. Assistant Prof., Department of Management, Tuyserkan Branch, Islamic Azad University, Tuyserkan, Iran. **E-mail: Taghvaei_reza@yahoo.com**
4. Assistant Prof., Department of Information Science and Epistemology, Hamedan Branch, Islamic Azad University, Hamadan, Iran. **E-mail: Behrooz.bayat@gmail.com**

**Article Information**

**Accepted:**
2023/05/01

**Receeived:**
2023/09/16

**Keywords:**

*Information Technology Security Management, Professional Ethics Policy.*

**Corresponding Author:**
Mansour Esmaeilpour

**Email:**
*Esmaeilpour@iauh.ac.ir*

## Abstract

**Background & Purpose:** Every organization should create a kind of information security management system according to the level of information in order to be able to identify and manage the information risks of the organization and the protection of information assets. Hence, in the current research, the design of the IT security management model with the approach of the professional ethics policies of the employees is discussed.

**Methodology:** The current research is an applied and developmental research and in terms of its nature, it is an exploratory research. This research was conducted using qualitative research method and thematic analysis strategy. In this research, field method and interview tools were used to collect data. Hence, 12 semi-structured interviews with chain sampling method (snowball) were conducted until reaching theoretical saturation with two groups of scientific and academic experts and executive experts. After implementing the text of the interviews in the Maxqda software, through the theme analysis technique based on Attride-Stirling approach, the research data were analyzed in three stages of basic, organizing and comprehensive themes.

**Findings:** Based on the data analysis, the research findings were organized into 6 overarching themes of professional ethics, commitment and responsibility, creativity and innovation, human resource management, human resource performance and organization structure, and 24 organizing themes and 244 basic themes.

**Conclusion:** The protection of organizational information requires a determined and persistent management, and proper monitoring can control possible unethical aspects and help ensure the security of information technology. Ethical behavior of employees is very important in the field of information technology security. If employees do not follow the policies and ethical principles, it may lead to data or systems security breaches. Behavioral monitoring can remind employees of the policy and put them on the correct behavioral path.

**Citation:** Esfandiar, Mostafa; Esmaeilpour, Mansour; Taghvaei, Reza and Bayat, Behrooz. (2023). The Management Model of Information Technology Security with the Approach of Professional Ethics Policies of Employees. *Journal of Air Defense Management*, 2(7), 193-214.

ISSN:2821-1588 htpps://www.jadm.khadu.ir

**فصلنامه علمی مدیریت دفاع هوایی**
دورهٔ ۲، شمارهٔ ۷
پاییز ۱۴۰۲
صص ۱۹۳-۲۱۴

**مقاله پژوهشی**

# الگوی مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای کارکنان

**مصطفی اسفندیار[۱]، منصور اسماعیل‌پور[۲]، رضا تقوایی[۳]، بهروز بیات[۴]**

۱. دانشجوی دکتری مدیریت فناوری اطلاعات، گروه مدیریت، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران. **رایانامه:** Mostafa.esfandyar@gmail.com

۲. دانشیار، گروه کامپیوتر، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران. **رایانامه:** Esmaeilpour@iauh.ac.ir

۳. استادیار، گروه مدیریت، واحد تویسرکان، دانشگاه آزاد اسلامی، تویسرکان، ایران. **رایانامه:** Taghvaei_reza@yahoo.com

۴. استادیار، گروه علم اطلاعات و دانش شناسی، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران. **رایانامه:** Behrooz.bayat@gmail.com

## اطلاعات مقاله

**تاریخ دریافت:**
۱۴۰۲/۰۲/۱۱

**تاریخ پذیرش:**
۱۴۰۲/۰۶/۲۵

**کلیدواژه‌ها:**

*مدیریت تأمین امنیت فناوری اطلاعات، خط‌مشی اخلاق حرفه‌ای.*

**نویسنده مسئول:**
منصور اسماعیل‌پور

**ایمیل:**
*Esmaeilpour@iauh.ac.ir*

## چکیده

**زمینه و هدف:** هر سازمانی باید نوعی سیستم مدیریت امنیت اطلاعات متناسب با سطح اطلاعاتی ایجاد کند تا بتواند ریسک‌های اطلاعاتی سازمان و حفاظت از دارایی‌های اطلاعاتی را شناسایی و مدیریت کند. بر این اساس، در پژوهش حاضر به طراحی الگوی مدیریت تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان پرداخته می‌شود.

**روش‌شناسی:** پژوهش حاضر از نوع، پژوهشی کاربردی و توسعه‌ای است و از نظر ماهیت از نوع تحقیقات اکتشافی است. این پژوهش با استفاده از روش تحقیق کیفی و راهبرد تحلیل مضمون انجام شد. در این پژوهش از روش میدانی و ابزار مصاحبه برای گردآوری داده‌ها استفاده شد. از این رو، تعداد ۱۲ مصاحبه نیمه‌ساختار یافته با روش نمونه‌گیری زنجیره‌ای (گلوله برفی) تا رسیدن به اشباع نظری با دو گروه خبرگان علمی و دانشگاهی و خبرگان اجرایی انجام شد. پس از پیاده‌سازی متن مصاحبه‌ها در نرم افزار مکس کودا، از طریق تکنیک تحلیل مضمون مبتنی بر رویکرد اتراید و استرلینگ، داده‌های پژوهش در سه مرحله مضامین پایه، سازمان‌دهنده و فراگیر تحلیل شدند.

**یافته‌ها:** بر اساس تحلیل داده‌ها، یافته‌های پژوهش در ۶ مضمون فراگیر اخلاق حرفه‌ای، تعهد و مسئولیت‌پذیری، خلاقیت و نوآوری، مدیریت منابع انسانی، عملکرد منابع انسانی و ساختار سازمان و ۲۴ مضمون سازمان‌دهنده و ۲۴۴ مضمون پایه سازماندهی شدند.

**نتیجه‌گیری:** حفاظت از اطلاعات سازمانی نیازمند یک مدیریت مصمم و پیگیر است و نظارت صحیح می‌تواند جنبه‌های غیراخلاقی احتمالی را کنترل نماید و به تأمین امنیت فناوری اطلاعات کمک کند. رفتار اخلاقی کارکنان در زمینه امنیت فناوری اطلاعات از اهمیت زیادی برخوردار است. اگر کارکنان از خط‌مشی‌ها و اصول اخلاقی پیروی نکنند، ممکن است به نقض امنیت داده‌ها یا سیستم‌ها منجر شود. پایش و نظارت رفتارها می‌تواند خط‌مشی کارکنان را به آن‌ها یادآوری کند و آن‌ها را در مسیر صحیح رفتاری قرار دهد.

**استناد:** اسفندیار، مصطفی؛ اسماعیل پور، منصور؛ تقوایی، رضا و بیات، بهروز. (۱۴۰۲). الگوی مدیریت تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان. *فصلنامه مدیریت دفاع هوایی*، ۲(۷)، ۱۹۳-۲۱۴.

## مقدمه

حرکت سریع کشورها در جامعه اطلاعاتی به رشد گسترده سیستم‌ها و خدمات اطلاعاتی و پیدایش نوع جدیدی از سازمان‌های مدرن مبتنی بر اطلاعات منجر شده است (آکین سانیا[1] و همکاران، ۲۰۲۳). با توجه به نقش اطلاعات به عنوان نوعی کالای ارزشمند در این سازمان‌ها، تهدیدات و خطرات امنیتی ناشی از محیط فناوری و اینترنت وجود دارد. چرا که برای یک سازمان، امنیت اطلاعات یک اولویت است. با رشد سریع فناوری اطلاعات، دسترسی به اطلاعات، پردازش و استفاده در سازمان در سطح جهانی آسان‌تر شده است. استفاده از سیستم‌های اطلاعاتی باعث بهبود کارایی، اثربخشی، شفافیت و پاسخگویی در رابطه با حکمرانی خوب می‌شود (آندیتا و آدیتیا[2]، ۲۰۲۳). بر این اساس، هر سازمانی باید یک سیستم مدیریت امنیت اطلاعات را بر اساس سطح اطلاعاتی ایجاد کند که بتواند ریسک‌های اطلاعاتی سازمان و حفاظت از دارایی‌های اطلاعاتی را مدیریت کند (رضوانی، ۱۳۹۷).

با توجه به اهمیت نقش فعلی اطلاعات در هر سازمان، استفاده از سیستم مدیریت امنیت اطلاعات برای فعال کردن، کنترل، تایید، حفاظت و بهبود امنیت اطلاعات موضوع مهمی به نظر می‌رسد، بنابراین سازمان‌ها و شرکت‌ها مطمئناً به دنبال پیاده‌سازی امنیت در سیستم اطلاعاتی هستند که این سیستم باید بر اساس نیازهای سازمان و اهمیت اطلاعات برنامه‌ریزی شده باشد و بتواند پشتوانه‌ای برای تأمین سرمایه اطلاعاتی باشد (سومرو[3]، ۲۰۱۶) چرا که عصر اطلاعات، تقاضاهایی را به شرکت‌هایی تحمیل می‌کند که مدت‌هاست به آن فکر نمی‌شد.

توسعه فناوری اطلاعات و ارتباطات ساختار جامعه را تغییر داده است. بسیاری از شرکت‌ها خود را برای استفاده مؤثر و کارآمد از فناوری اطلاعات و ارتباطات آماده می‌کنند (اله رخا[4]، ۲۰۲۳). شکی نیست که نه تنها ایجاد تغییرات در حوزه‌های مختلف سازمان و تغییرات محیطی و استفاده از ابزارهایی که عهده‌دار آن زمان هستند با توسعه فناوری ضروری است، بلکه زندگی سازمان به این مشکل مهم در دنیای پرتلاطم امروز وابسته است (وظیفه و همکاران،۱۳۹۷). فناوری اطلاعات با استفاده از علوم مختلف توانسته است در مدت زمان کوتاهی اطلاعات مهمی را در اختیار انواع جامعه قرار دهد. این فناوری کشورهای

---

1. Akinsanya
2. Andita and Aditya
3. Soomro
4. Allahrakha

مختلف را در سراسر جهان به هم متصل کرده است (دیرانی[1] و همکاران، ۲۰۲۳). با این حال، اگر هنگام تماشای پیشرفت و یادگیری آن به ایمنی او توجه نکنیم، می‌تواند بسیار خطرناک باشد. از سوی دیگر، با افزایش توسعه فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری توانایی تبادل اطلاعات افزایش یافته و روش‌های اجرای تهدیدات مذکور دشوارتر می‌شود (نیک‌ران[2] و همکاران، ۲۰۱۷). از این‌رو، حفظ ایمنی فضای تبادل اطلاعات از مهمترین اهداف توسعه فناوری اطلاعاتی و ارتباطی محسوب می‌شود. محققان بر این باورند که اکثر سازمان‌ها بدون توجه به 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 خسارت بیشتری متحمل می‌شوند ولی متأسفانه همچنان این روش را ادامه می‌دهند (ایمت[3]، ۲۰۱۵). سیستم اطلاعات به سیستم‌های سخت‌افزاری، نرم‌افزاری، داده‌ها، کنترل‌ها، رویه‌ها و افراد درون سازمان بستگی دارد همه این عناصر به مدیریت کافی و سیستم مدیریت اطلاعات کارآمد برای حفظ اطلاعات محرمانه سازمان مربوطه نیاز دارند و این ویژگی‌ها با کنترل‌های امنیتی خاصی مورد محافظت قرار می‌گیرند (عیدی و همکاران، ۱۴۰۲).

امروزه رعایت اخلاق حرفه‌ای توسط مدیران به عنوان یکی از عمده‌ترین متغیر در موفقیت سازمان‌ها شمرده می‌گردد. در دهه‌های اخیر مدیران سازمان‌ها به اهمیت تزریق اخلاق حرفه‌ای در شریان‌های حیاتی سازمان‌ها بیش از پیش پی برده‌اند و اکنون خوب می‌دانند که عنصر اخلاق به عنوان یکی از عوامل ثبات سازمان و نیل به اهداف غایی آن است. همچنین یکی از اساسی‌ترین اصول ایجاد ارتباطات سالم و اثرگذار در میان کارکنان سازمان‌ها، رعایت اصول اخلاق حرفه‌ای توسط مدیران سازمان‌هاست (دوستی، ۱۴۰۲). اما در جهان امروز به دلیل گسترش روزافزون فناوری و برقراری وسیع ارتباطات در محیط مجازی و عدم توجه به ابعاد معنوی و روحی انسان و عدم آشنایی با اصول و تکنیک‌های مدیریت و رفتار حرفه‌ای، بسیاری از اصول اخلاقی در میان مدیران و کارکنان سازمان‌ها مورد غفلت واقع شده است و عدم توجه به ضوابط اخلاقی از سوی آنان باعث بروز بسیاری از مشکلات موجود در سازمان‌ها شده است. (شفیع پور و دیگران، ۱۳۹۶). یکی از جنبه‌های مهم برای مدیریت امنیت اطلاعات، افزایش آگاهی کاربران از امنیت اطلاعات است.

---

[1]. Dhirani
[2]. Nikrerk
[3]. Emmett

آگاهی مردم از امنیت اطلاعات به تغییر رفتار و تقویت تدابیر امنیتی مناسب منجر می‌شود و افراد را قادر می‌سازد تا امنیت فناوری اطلاعات را مورد توجه قرار دهند که به تدریج به فرهنگ سازمان‌ها تبدیل خواهد شد (زنجیرچی و همکاران، ۱۳۹۳). سیستم‌های اطلاعاتی و برنامه‌های کاربردی سازمان معمولاً سیستم‌های پیچیده‌ای هستند که بسیاری از وظایف را در سازمان در بر می‌گیرند. از آنجایی که سازمان معمولاً به شدت به این سیستم‌ها وابسته است، هر نوع عاملی که عملکرد آنها را مختل کند، می‌تواند صدمات جدی و جبران‌ناپذیری به سازمان وارد کند. مشکلات امنیتی در سیستم‌های اطلاعاتی یک مشکل رایج است و به دلیل استفاده از سیستم‌های اطلاعاتی و کاربردی فراوان سازمان، مقوله امنیتی این سیستم‌ها از اهمیت بالایی برخوردار است (ساها[1]، ۲۰۱۸) و حیات سازمان‌ها ارتباط تنگاتنگی با سیستم‌های اطلاعاتی آنها دارد. سیستم‌های اطلاعاتی همیشه در معرض خطر سرقت داده‌ها، تغییر داده‌ها و قطع خدمات هستند. برای حل یک مشکل امنیتی، یک شرکت باید از دانش، فناوری و قوانین سازمانی گسترده استفاده کند و اطمینان حاصل کند که شرکت نه تنها بر راه‌حل‌های فنی تمرکز می‌کند، بلکه آنها را نیز به کار می‌گیرد (یزدان مهر و همکاران، ۲۰۲۳). معرفی موفقیت‌آمیز فناوری‌های جدید، دولت را قادر می‌سازد تا خدمات عمومی کارآمدتری را به شهروندان ارائه دهد و با توجه به اهمیت نقش مدیریت امنیت فناوری اطلاعات در حفاظت از اطلاعات سازمان، یکی از عواملی که می‌تواند به تغییر در ارزش‌های اخلاقی سازمان منجر شود، اجرای سیاست‌ها و برنامه‌های مدیریت امنیت اطلاعات است (استرگیو[2] و همکاران، ۲۰۱۸). بنابراین اهمیت تحقیق جامع در زمینه اخلاق حرفه‌ای و کسب و کار در حوزه مدیریت امنیت فناوری اطلاعات مشخص می‌شود.

شواهد زیادی وجود دارد که نشان می‌دهد کمبود فناوری اطلاعات شرکت‌ها و صنایع را از بسیاری از فرصت‌های سودآور محروم می‌کند و به دلیل ناتوانی در دستیابی به مزیت اقتصادی و به ویژه اطلاعاتی، موقعیت و سهم بازار خود را کاملاً از دست می‌دهد. هدف از مدیریت امنیت اطلاعات در سازمان، حفاظت از دارایی‌های سازمان (نرم‌افزار، سخت‌افزار، اطلاعات، ارتباطات و پرسنل) در برابر هرگونه تهدید (از جمله دسترسی غیرمجاز به اطلاعات، خطرات و خطرات ناشی از محیط و سیستم و کاربران) است. در این شرایط خلأ مدل پیاده‌سازی مدیریت امنیت فناوری اطلاعات در بین سازمان‌های ایرانی به وضوح قابل مشاهده است. استانداردها، چارچوب‌ها و تجربیات بسیاری در عرصه بین‌المللی ارائه شده

---

[1]. Saha
[2]. Stergiou

است. مرور مدل‌های موجود در پژوهش‌های یل هورسا و همکاران (۲۰۲۲)، آل–قدمدی و همکاران[۱] (۲۰۲۲)، رازیکین و سویتو[۲] (۲۰۲۲)، کانگ و همکاران[۳] (۲۰۲۲)، آگروال و دهرکاری[۴] (۲۰۲۲)، ویمرکاتی و همکاران[۵] (۲۰۲۲)، سیملامبو و همکاران[۶] (۲۰۲۱)، ماندال و کاندان[۷] (۲۰۲۱)، کروتو و جانسون[۸] (۲۰۲۲)، دی زویاس[۹] (۲۰۲۲)، منبارو[۱۰] (۲۰۲۱)، فیناروس[۱۱] (۲۰۲۲) و لی و چو (۲۰۲۱) نشان می‌دهد که با توجه به وجود شکاف‌های پژوهشی در حوزه مدل‌سازی ارتباط بین راهبرد خدمات تأمین امنیت فناوری اطلاعات؛ طراحی خدمات تأمین امنیت فناوری اطلاعات؛ انتقال خدمات تأمین امنیت فناوری اطلاعات؛ عملیات خدمات تأمین امنیت فناوری اطلاعات؛ بهبود مستمر خدمات تأمین امنیت فناوری اطلاعات و اجرای نظام مدیریت امنیت اطلاعات، نبود مدلی جهت ارائه توصیه‌هایی به مدیران برای تصمیم‌گیری جهت مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای کارکنان احساس می‌شود.

اخلاق حرفه‌ای سازمان‌ها یک ضرورت در مدیریت منابع انسانی و رفتار سازمانی است. اخلاق حرفه‌ای برای تشویق افراد سازمان برای استفاده از تفکر انتقادی و استدلال منطقی در حین انتخاب مستقل از ضروریات است و به عنوان راهنمای وجود انسان عمل می‌کند. سازمان‌ها باید ویژگی‌های اخلاق حرفه‌ای مانند مسئولیت اجتماعی، نظم و انضباط، وجدان کاری، تکریم ارباب رجوع، ارزش‌های اخلاقی، حقوق شهروندی، منشور اخلاقی، صداقت و راستگویی، انصاف و برابری، امانت‌داری، وفاداری، روحیه مشارکت، اعتماد و تعهد، ایجاد تعامل با یکدیگر و ... را تعریف نموده و برای تحقق آن فرهنگ‌سازی نمایند که این امر از طریق طراحی الگوی مدیریت تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان امکان‌پذیر است. با بررسی ادبیات پژوهش مشخص شد که تاکنون پژوهشی در رابطه با مدیریت تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان صورت نگرفته است. با این حال، حلقه مفقوده عدم وجود مدلی گام به گام است که شهرداری‌های کشور بسته به شرایط خود از آن استفاده کنند. بنابراین مسأله اصلی

---

1. AlGhamdi, et al
2. Razikin and Soewito
3. Kang, et al
4. Aggarwal and Dhurkari
5. Vimercati, et al
6. Semlambo, et al
7. Mandal and Chandan
8. Krotov and Johnson
9. De Zoysa
10. Menbarrow
11. Finuras

تحقیق عبارت است از اینکه الگوی مدیریت تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور چگونه است؟.

## پیشینهٔ پژوهش

**مدیریت امنیت اطلاعات؛** سیستم اطلاعات به سیستم‌های سخت‌افزاری، نرم‌افزاری، داده‌ها، کنترل‌ها، رویه‌ها و افراد درون سازمان بستگی دارد همه این عناصر به مدیریت کافی و سیستم مدیریت اطلاعات کارآمد برای حفظ اطلاعات محرمانه سازمان مربوطه نیاز دارند و این ویژگی‌ها با کنترل‌های امنیتی خاصی مورد محافظت قرار می‌گیرند (عیدی و همکاران، ۱۴۰۲).

در عصر امروز، اطلاعات یک منبع استراتژیک و یک قابلیت کلیدی شامل سایر عناصر کلیدی امنیت اطلاعات از جمله فرآیندها و پرسنل است و در کنار توجه به تأمین امنیت اطلاعات باید به جو اخلاقی حاکم بر سازمان نیز توجه ویژه‌ای شود چرا که اگر اخلاق حرفه‌ای کارکنان همسو با سازمان باشد بهتر می‌توانند از اطلاعات سازمان و موارد امنیتی آن محافظت کنند. از این رو موضوع امنیت اطلاعات و اخلاق حرفه‌ای کارکنان در دستور کار دولت‌ها قرار گرفته است تا از استفاده صحیح از این منبع اطمینان حاصل شود. ترویج اخلاق در فناوری اطلاعات هدف‌های عمده مانند احترام اصیل و نامشروط آدمی، آزادی فردی، عدالت اجتماعی و امانت‌داری را دارا است (دوستی، ۱۴۰۲).

سیستم‌های اطلاعاتی همیشه در معرض خطر سرقت داده‌ها، تغییر داده‌ها و قطع خدمات هستند. برای حل یک مشکل امنیتی، یک شرکت باید از دانش، فناوری و قوانین سازمانی گسترده استفاده کند و اطمینان حاصل کند که شرکت نه تنها بر راه‌حل‌های فنی تمرکز می‌کند، بلکه آنها را نیز به کار می‌گیرد (یزدان مهر و همکاران، ۲۰۲۳).

به موازات گسترش شبکه محلی و سراسری، تهدیدات و سرقت و تخریب اطلاعات نیز افزایش یافته است؛ به طوری که شاید یکی از مهمترین مسائل در عصر اطلاعات، حفاظت و امنیت آن است (میوالد، ۲۰۰۴). بحث مدیریت امنیت اطلاعات به دلیل پیچیدگی زیاد، با مسائل بحث‌انگیز زیادی مواجه می‌شود که این مباحث در راستای فراهم آوردن چارچوب، روش و فناوری‌هایی برای بهبود پیاده‌سازی امنیت اطلاعات در سازمان است (چاو، ۲۰۰۵).

آلفانتوخ (۲۰۰۹) یازده پارامتر اساسی زیر را برای مدیریت امنیت اطلاعات مطرح می‌کند (قربان زاده و همکاران،۱۳۹۶)؛

**سیاست‌های امنیت اطلاعات:** اینکه چگونه یک موسسه قصد و نیت خود را با تأکید بر امنیت اطلاعات بیان می‌دارد، بدین معنی است که در بدنه اداری آن سازمان تمایل به

امن‌سازی اطلاعات قابل مشاهده است. این سیاست‌ها خط‌مشی مدیریت و کارکنان را مشخص کرده و اولویت تلاش‌های آنان را شکل می‌دهد.

**مدیریت ارتباطات و عملیات:** سیاست تعریف شده برای امنیت سازمان جهت کاهش ریسک امنیت و اطمینان از طریق ارزیابی صحیح فرآیندهای عملیاتی، کنترل‌ها، مسئولیت‌های تعریف شده دقیق و ... است.

**سیستم‌های اطلاعاتی مالکیت، توسعه و مدیریت:** فرآیندی تجمیعی که مرزها و سیستم‌های اطلاعاتی فنی را تعریف کرده و با مالکیت و توسعه آخرین نگهداشت سیستم‌های اطلاعاتی شروع می‌شود.

**کنترل دسترسی:** سیستمی است که احراز هویت را برای کنترل دستیابی به محدوده‌ها و منابع موجود در یک موجودیت فیزیکی یا همان سیستم‌های اطلاعاتی بر پایه کامپیوتر را امکان‌پذیر می‌سازد.

**سازماندهی امنیت اطلاعات:** ساختاری متعلق به سازمان است که اجرای امنیت اطلاعات شامل الزامات مدیریتی برای امنیت اطلاعات، هماهنگی امنیت اطلاعات، فرآیند احراز هویت برای امکانات پردازشی اطلاعاتی را سازماندهی می‌نماید و شامل دو شاخه کلی داخل سازمانی و شرکای خارجی است.

**مدیریت دارایی‌ها:** مبتنی بر این ایده شناسایی، پیگیری، دسته‌بندی و تنظیم مالکیت برای اغلب دارایی‌های سازمانی است و از این جهت مهم است که اطمینان خاطر حاصل شود که دارایی‌ها به طور مناسبی مورد حفاظت قرار خواهند گرفت.

**مدیریت حوادث امنیت اطلاعات:** برنامه‌ای است که برای حوادث پیش‌بینی و فراهم شده است. از دیدگاه مدیریتی، شناسایی منابع مورد نیاز برای جلوگیری از بروز حوادث امنیتی است. مدیریت مناسب حوادث از بروز رخدادهای امنیتی در آینده جلوگیری می‌نماید.

**مدیریت استمرار کسب و کار:** برای اطمینان از استمرار عملیات تجاری در شرایط غیر نرمال است. برنامه‌ها آمادگی مؤسسات را برای بازیابی سریع در شرایط خاص تضمین می‌نمایند. چنین مدیریتی باعث کاهش تأثیر شرایط نامناسب شده و امکانات لازم را برای سهولت عملیات حین و بعد از شرایط اضطراری فراهم می‌سازند.

**امنیت منابع انسانی:** برای اطمینان از اینکه تمام کارکنان اعم از پیمانکاران و کاربران داده‌های حساس همگی ملزم به درک نقش و مسئولیت کارها و وظایف خود بوده و در صورت فسخ قرارداد کاری، دسترسی به منابع خاتمه می‌یابد.

**امنیت فیزیکی و محیطی:** معیار اندازه‌گیری برای حفاظت از سیستم‌ها، ساختمان‌ها و زیرساخت‌های مرتبط برای مقابله با تهدیدات درگیر با محیط فیزیکی بوده، به طوری که

ساختمان‌ها و اتاق‌هایی که مسئول نگهداری اطلاعات و سیستم‌های اطلاعاتی هستند قابلیت حفاظت از آن محیط را داشته باشند. این کار برای جلوگیری از آسیب دیدن یا دسترسی غیرمجاز به سیستم‌های اطلاعاتی انجام می‌گیرد.

**انطباق:** مسائل این بخش به دو حوزه تقسیم می‌شوند؛ بخش اول بحث انطباق با قوانین متعددی است که در داخل هر سازمان به صورت مقررات و نیازمندی‌های سازمانی وجود دارد. بخش دوم نیز انطباق با سیاست‌های امنیت اطلاعات، استانداردها و فرآیندها است.

**اخلاق حرفه‌ای؛** اخلاق حرفه‌ای مسئولیت های اخلاقی سازمان در قبال محیط مستقیم و غیرمستقیم است و بر اصل حق مردم استوار است؛ یعنی «محیط حق دارد و سازمان وظیفه». اخلاق حرفه‌ای رفتار ارتباطی سازمان با محیط بر اساس حقوق و تعهدات و وظایف است (ریابوآ[1] و همکاران،۲۰۲۱). اخلاق حرفه‌ای شاخه‌ای از اخلاق کاربردی است که به مباحث اخلاق در حرفه می‌پردازد و مفهومی بسیار وسیع‌تر از اخلاق کسب وکار دارد. اخلاق می‌تواند در زندگی فردی- شخصی باشد و می‌تواند در زندگی فردی- شغلی باشد. اخلاق کار و یا اخلاق شغلی بخشی از اخلاق حرفه‌ای است. بخش بزرگی از اخلاق حرفه‌ای فراتر از زندگی فردی و شغلی با عملکرد اخلاق سازمان‌ها سروکار دارد؛ بنابراین، مفهوم اخلاق حرفه‌ای، اخلاق در زندگی فردی- شغلی و اخلاق سازمانی را نیز در بر می‌گیرد (صانعی و یاری، ۱۳۹۳). اخلاق حرفه‌ای، مجموعه‌ای از قواعد و رویه‌هایی است که در حوزه‌های کاری، تجاری و سازمانی باعث ارتقا عملکرد کاری سازمان می‌شود. اخلاق حرفه‌ای دربردارنده مجموعه‌ای از هنجارها، ارزش‌ها و الگوهای رفتاری است که توسط افراد و سازمان‌ها مورد حمایت است. همچنین اخلاق حرفه‌ای مجموعه از باید و نبایدهای سازمانی است که به منظور ارتقای سطح کیفی و کمی سازمان‌ها توسط مدیران تنظیم شده است (کارالینا[2] و همکاران، ۲۰۲۱).

## پیشینه تجربی

سلحشوری و همکاران (۱۴۰۱) در مطالعه بررسی و تبیین امنیت داده‌ها بیان نمودند که امنیت اطلاعات و ایمن‌سازی شبکه‌های رایانه‌ای از جمله عناصری بود که نمی‌توان آن را مختص یک فرد یا سازمان در نظر گرفت. وجود ضعف امنیتی در شبکه‌های رایانه‌ای و اطلاعاتی، عدم آموزش و توجیه صحیح همه کاربران صرف‌نظر از مسئولیت شغلی آنان

---

[1]. Riabova
[2]. Carauleanu

نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورالعمل‌های لازم برای پیش‌گیری از نقایص امنیتی، عدم وجود خط‌مشی‌های مشخص و مدون با هدف برخورد مناسب و به موقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه همه کاربران رایانه در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد.

طاهری‌راد و ویسی (۱۴۰۱) در پژوهش پیاده‌سازی مرکز عملیات امنیت در سازمان فناوری اطلاعات و ارتباطات شهرداری شیراز با راه‌اندازی مرکز عملیات امنیت شهرداری، اثرات این مرکز بر بهبود فرآیندها و ارتقای سطح امنیت سازمان را بررسی نمودند. راه‌اندازی این مرکز با مدل‌سازی تهدید آغاز و طی این فرآیند، مدیران شبکه و امنیت فناوری اطلاعات گرد هم آمده تا تهدیدات سایبری کلیدی را تشخیص داده و اولویت‌بندی نمایند. سپس شکل فرضی آن‌ها در داده‌های ماشینی به شکل مدل درآورده و در نهایت تعیین شد چطور می‌توان آن‌ها را شناسایی و اصلاح نمود.

وظیفه، مهدی و وکیلی (۱۳۹۷) تحقیقی با عنوان الگوی امکان‌سنجی و استقرار اثربخش سیستم مدیریت امنیت اطلاعات بر مبنای روش فراترکیب انجام داده‌اند. محقق با استفاده از روش فراترکیب، بازنگری دقیق و عمیق در موضوع انجام داده است و یافته‌های پژوهش‌های کیفی و کمی مرتبط را ترکیب کرده است. در این راستا ۱۱۸ پژوهش در زمینه مدیریت امنیت اطلاعات و سیستم‌های اطلاعاتی ارزیابی شده که در پایان ۵۵ پژوهش انتخاب و با تحلیل محتوای (اسنادی- کتابخانه‌ای) آن‌ها، ابعاد و کدهای مربوطه استخراج و میزان اهمیت و اولویت هریک با استفاده از آنتروپی شانون تعیین شده است. بر اساس یافته‌های تحقیق، 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 داشت است. در نهایت، پس از طی گام‌های پژوهش، الگوی تعیین و استقرار اثربخش سیستم مدیریت امنیت اطلاعات در سه لایه شناسایی، ساختار اجرا و طراحی برنامه حمایتی سیستم مدیریت امنیت اطلاعات ارائه گردیده است.

جعفری و شمسی (۱۳۹۵) تحقیقی با عنوان بررسی عوامل موثر بر رعایت اخلاق فناوری اطلاعات انجام داده اند. مدل پژوهش بر اساس تئوری رفتار برنامه ریزی شده توسعه یافته و متغیر جنسیت به عنوان متغیر تعدیل‌گر در نظر گرفته شده است. جامعه آماری پژوهش، شامل دانشجویان دانشگاه‌های تهران و شهید بهشتی بوده است. جمع‌آوری داده‌های پژوهش با استفاده از پرسشنامه انجام و فرضیه‌ها با استفاده از مدل‌یابی معادلات ساختاری آزمون شده است. یافته‌های پژوهش نشان داد که سیستم اعتقادی، ارزش‌های

شخصی، محیط شخصی، خودباوری و محیط قانونی به طور غیرمستقیم و نگرش، هنجار ذهنی و نیت رفتاری به طور مستقیم بر رعایت اخلاق اطلاعات تاثیر مثبت و معناداری دارند و جنسیت دانشجویان برخی از این روابط را تعدیل می‌کند.

در مطالعه هیل هورست و همکاران (۲۰۲۲) به شناسایی و بررسی معیارهای افزایش کارایی در ارائه خدمات عمومی از طریق فناوری اطلاعات در شهرداری‌ها اقدام گردید. در حقیقت نتایج اصلی افزایش کارایی فناوری اطلاعات در شهرداری‌ها شامل معیارهایی از قبیل تولید خروجی‌های خدمات عمومی با هزینه کمتر، تولید خروجی‌های خدمات عمومی در زمان کمتر و تولید خروجی‌های خدمات عمومی با کیفیت بهتر بود.

در مطالعه اگاروال و دورکاری[1] (۲۰۲۲) به تدوین مدلی جهت تحلیل ارتباط بین استرس شغلی کارکنان و رفتار عدم انطباق خط‌مشی امنیت اطلاعات بر اساس روش فراتحلیل اقدام شد. رفتارهای اثرگذار بر خط‌مشی امنیت اطلاعات شامل پیاده‌سازی طرح امنیت اطلاعات و پشتیبانی امنیت فضای تبادل اطلاعات سازمان بود.

## روش‌شناسی پژوهش

پژوهش حاضر از نوع، پژوهشی کاربردی و توسعه‌ای است و از نظر ماهیت و هدف نیز از در طیف پژوهش‌های اکتشافی قرار دارد که در آن از راهبرد تحلیل مضمون استفاده شد. برای این منظور ابتدا با استفاده از مطالعات کتابخانه‌ای به بررسی مبانی نظری و پیشینه پژوهش پرداخته شد و در ادامه با استفاده از بررسی‌های میدانی و مصاحبه با خبرگان، نسبت به طراحی الگو «مدیریت تأمین امنیت فناوری اطلاعات با رویکرد خط‌مشی‌های اخلاق حرفه‌ای کارکنان» اقدام شد. در این راستا مصاحبه‌های نیمه ساختاریافته بر مبنای قاعده اشباع نظری صورت گرفت و با استفاده از روش نمونه‌گیری گلوله برفی با جامعه‌ی آماری دو گروه خبرگان علمی و دانشگاهی و گروه دوم خبرگان اجرایی انتخاب شدند. در این خصوص پس از انجام ۱۲ مصاحبه، مفهوم جدیدی که واجد ارزش افزوده باشد، یافت نشد و مصاحبه‌ها متوقف گردید.

اقدامات زیر برای ارتقای روایی پژوهش انجام شد؛ افرادی برای شرکت در مطالعه انتخاب شدند که دارای تخصص و تجربه کافی در خصوص موضوع تحقیق بوده‌اند، جمع‌آوری، تحلیل و تفسیر داده‌های کیفی توسط پژوهشگر که سوابق مشخصی در خصوص در هم تنیدگی و تجربه زیسته با موضوع تحقیق و سنت‌های کیفی در تحقیق دارد انجام

---

[1]. Aggarwal and Dhurkari

شده است، استاد راهنما سابقه اجرایی، راهنمایی، مشاوره و انتشار مطالعات متعدد در سنت کیفی داشته و فرایند تحقیق تحت نظارت مستمر استاد راهنما انجام شده است، فرایند انجام مطالعه کیفی به تفصیل گزارش شده است، ارزش‌ها و علائق پژوهشگر که می‌تواند بر جریان جمع‌آوری، تحلیل و تفسیر داده‌ها تاثیرگذار باشد گزارش شده است، ملاحظات اخلاقی در تحقیق همچون شرکت داوطلبانه در مطالعه، ضبط مصاحبه با اخذ رضایت آگاهانه و... در نظر گرفته شده است و جمع‌آوری داده‌ها تنها پس از اطمینان از رسیدن به اشباع نظری متوقف گردیده است.

جهت بررسی پایایی پژوهش از ضریب کاپا استفاده شد. بر اساس تحلیل داده‌ها، شاخص کاپا برابر با مقدار ۰.۷۸ به دست آمد که نشان‌دهنده اعتبار کدهای مستجرجه بود.

**جدول ۱. ضریب توافق کاپا**

| 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 به دست 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 مربوط به آن مقوله در کنار هم قرار گرفته و تحلیل شد. در ادامه پس از پیاده‌سازی متن مصاحبه‌ها در نرم افزار مکس‌کودا با استفاده از راهبرد پژوهشی تحلیل مضمون و شیوه‌ی کدگذاری به طراحی الگوی پژوهش اقدام گردید.

## یافته‌های پژوهش

جهت تدوین مدل مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور از طریق مصاحبه با خبرگان اقدام شد. بعد از پاسخگویی خبرگان به فرم‌های مصاحبه، کدهای تحقیق با روش تحلیل مضمون (تم) استخراج شد. در واقع، شاخص‌های گزارش شده در جدول ۲ کدهایی هستند که از پاسخ خبرگان به سؤالات فرم مصاحبه استخراج شده است. هر یک از شرکت‌کنندگان مهمترین مؤلفه‌های مدل مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور را بیان کردند. با توجه به چارچوب و مراحل 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 که در جدول ۲ نمایش داده می‌شود.

**جدول ۲. شبکه مضامین مدل مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور**

| مضامین فراگیر | مضامین سازمان دهنده | مضامین پایه |
|---|---|---|
| | احترام و کرامت | 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 |
| | | 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 مسئولیت پذیری | 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 |

| مضامین فراگیر | مضامین سازمان دهنده | مضامین پایه |
|---|---|---|
| | | فضای خلاق |
| | | اعطای اختیار عمل |
| | | تدوین آیین نامه‌هایی 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 سازمان‌های یادگیرنده |
| | | شناسایی و حذف موانع داخلی |
| | فردی | نگاه مثبت به مشکلات در جهت بهبود امور و ارائه 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 فعالیت‌های آموزشی |
| | | برگزاری کارگاههای آموزشی و توجیهی |
| | | پرورش و رشد اخلاق پرسنل و اخلاق مداری در انجام وظایف |
| | | آموزش کارکنان |
| | توسعه حرفه‌ای منابع انسانی | اجرای برنامه‌هایی 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 |
| | | مزیت رقابتی |
| | | 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 فرصت‌هایی برای فراگیران ایجاد کنند تا محتوای آموزشی را در کارشان به کار گیرند |
| | | اجرای راه کارهای افزایش کارایی و عملکرد در سازمان |
| | | برگزاری دوره‌های آموزشی اخلاقی و مذهبی برای پرسنل |
| | | حرکت به سوی رشد و ارتقای کارمندان |
| | | شناسایی ضعف‌ها و قوت‌های فردی با ارزیابی شایستگی |
| | | خوداتکایی |
| | | داشتن پشتکار و نداشتن هراس از نتیجه کار |
| | انگیزش | اجرای برنامه‌هایی با هدف انگیزش |
| | | ایجاد علاقه به کار |

| مضامین فراگیر | مضامین سازمان دهنده | مضامین پایه |
|---|---|---|
| | | 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 |
| | | 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 آن‌ها |
| | | پاداش به موفقیت‌ها و به شکست‌ها به فراخور |
| | مشارکت | استفاده از برنامه‌های 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 تیمی‌ها |
| | | 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 | عملکرد وظیفه ای |
| | | خویشتنداری، شکیبایی و خودداری از شکایت در ناگواری‌ها و سختی‌ها |
| | | فرهنگ مداری |
| | | ظرفیت پذیرش رویدادهای گوناگون |
| | | خستگی ناپذیری |
| | | خوش قولی |
| | | خلوص نیت |

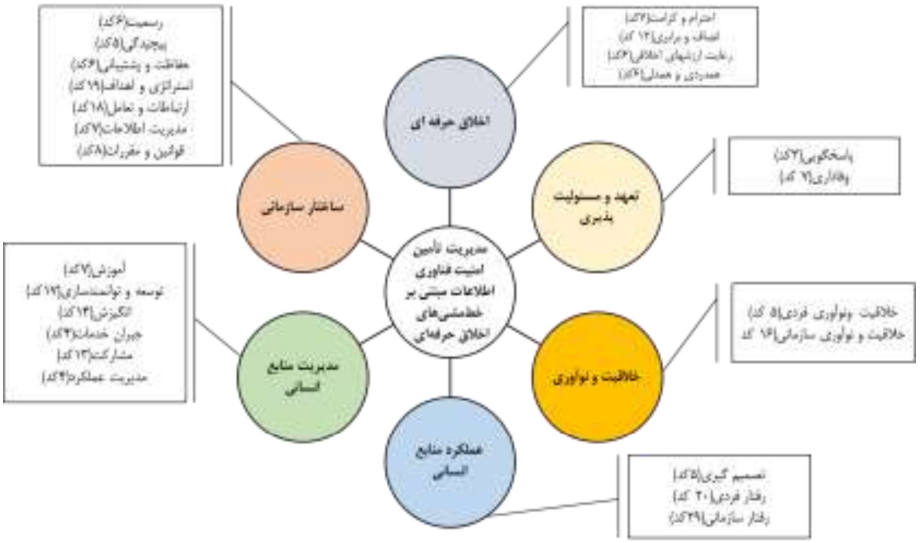
| مضامین فراگیر | مضامین سازمان دهنده | مضامین پایه |
|---|---|---|
| | | خوش اخلاقی |
| | | صبر و حوصله |
| | | پرهیز از حسد |
| | | هدفمنـــد بودن در زندگی |
| | | اخلاق پسندیده |
| | | داشتن صبر و شکیبایی |
| | | تکامل |
| | | تخصص |
| | | نفوذ کلام |
| | | تهذیب نفس |
| | | پرهیز از شتابزدگی |
| | | 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 شایستگی و تخصص و تحصیلات و آموزش 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 |

| مضامین فراگیر | مضامین سازمان دهنده | مضامین پایه |
|---|---|---|
| | | بهینه سازی تعداد کارکنان |
| | | قرار دادن مبنای پاداش‌ها و مجازات‌ها بر اصل شایسته سالاری |
| | پیچیدگی | عدم تمرکزگرایی سازمانی و کاهش هزینه‌ها |
| | | اتوماسیون و کاهش عملیات دستی |
| | | افزایش سرعت و سادگی کار |
| | | سیستم‌های یکپارچه اطلاعات مدیریت با هدف استفاده بهینه از فناوری ارتباطات و اطلاعات |
| | | توجه به جزئیات موجود در فرآیند استخدام، ارزیابی عملکرد و... |
| | حفاظت و پشتیبانی | مدیریت از راه دور |
| | | امنیت اطلاعات |
| | | حفاظت از سرورها |
| | | خدمات پشتیبانی اختصاصی |
| | | ایمنی سامانه از اشتباهات عمدی |
| | استراتژی و اهداف | طرّاحی فرایند خطاناپذیری کار |
| | | شاخص‌ها و اهداف سازمانی |
| | | بکارگیری افراد با استعداد و ایمان کاری و دریافت 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 |
| | | تعامل و همکاری |
| | | فراهم آوردن تسهیلات و امکانات رفاهی جهت پرسنل سازمان |
| | | برخورد قانونی و موثر با پرسنل |
| | | اخلاق مناسب مدیران جهت اخذ اطلاعات از پرسنل |
| | | تخصص مدیریت |
| | | الگو بودن برای کارکنان |
| | | برقراری ارتباط چشمی |
| | | همدردی با کارمندان |
| | | برخورد قاطعانه در صورت لزوم |

| مضامین فراگیر | مضامین سازمان دهنده | مضامین پایه |
|---|---|---|
| | | اعتماد کارکنان به مدیرشان |
| | | رفتاری صادقانه و شفاف با همکاران و پرهیز از ریاکاری |
| | | احترام به افکار دیگران |
| | مدیریت اطلاعات | یکپارچه سازی اطلاعات |
| | | 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 ابزارهای 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 |

همان‌طور که جدول ۲ نشان می‌دهد، مدل مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور بر اساس نظرات ۱۲ نفر از خبرگان در دسته بندی‌های مختلف و در ۲۴۴ کد باز آورده شده‌اند که ۶ بعد (اخلاق حرفه‌ای، تعهد و مسئولیت‌پذیری، خلاقیت و نوآوری، مدیریت منابع انسانی، عملکرد منابع انسانی و ساختار سازمان) وجود دارند و هر کدام نیز دارای کدهای محوری مختص خود هستند. به طوری که بعد اخلاق حرفه‌ای مجموعاً با ۳۱ کد باز دارای چهار کد محوری احترام و کرامت با ۷ کد، انصاف و برابری با ۱۲ کد، رعایت ارزش‌های اجتماعی با ۶ کد و همدردی و همراهی با دیگران با ۶ کد است. همچنین بعد تعهد و مسئولیت‌پذیری مجموعاً با ۱۰ کد باز دارای دو کد محوری پاسخگویی با ۳ کد و وفاداری با ۷ کد است. بعد خلاقیت و نوآوری مجموعاً با ۲۱ کد باز دارای دو کد محوری سازمانی با ۱۶ کد و فردی با ۵ کد است. بعد مدیریت منابع انسانی مجموعاً با ۵۹ کد باز دارای شش کد محوری آموزش با ۷ کد، توانمندسازی و ارتقاء مهارت با ۱۷ کد، انگیزش با ۱۴ کد، جبران خدمات با ۴ کد، مشارکت با ۱۳ کد و مدیریت عملکرد با ۴ کد است. همچنین بعد عملکرد منابع انسانی مجموعاً با ۵۴ کد باز و سه کد محوری تصمیم گیری با ۵ کد، رفتار فردی با ۲۰ کد و رفتار سازمانی با ۲۹ کد است. در نهایت بعد ساختار سازمان مجموعاً با ۶۹ کد باز دارای هفت کد محوری رسمیت با ۶ کد، پیچیدگی با ۵ کد، حفاظت و پشتیبانی با ۶ کد، استراتژی و اهداف با ۱۹ کد، ارتباطات و تعامل با ۱۸ کد، مدیریت اطلاعات با ۷ کد و رعایت نظم و مقررات با ۸ کد است. در شکل ۱ مدل نهایی مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق

حرفه‌ای کارکنان در شهرداری‌های کشور رسم شده است.




**شکل۲. الگوی مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای**

## بحث و نتیجه‌گیری

در عصری که سازمان‌ها با انبوهی از داده و اطلاعات سروکار دارند و نگهداری و حفظ آنها به عنوان یکی از دارایی‌های نامشهود سازمان اهمیت روزافزونی پیدا کرده است، اخلاق حرفه‌ای کارکنان نه تنها در عملکرد شغلی آنها بلکه در برخورد با مدیریت داده و اطلاعات سازمان ضرورت پیدا کرده است. ضرورت اخلاق حرفه‌ای در منشور اخلاقی سازمان از آنجایی است که در عصر کنونی جهانی شدن، سطح رقابت رو به افزایش است و تنها کسانی که آماده و با منابع کافی و ذهنیت حرفه‌ای هستند می‌توانند شکوفا شوند و دوام بیاورند. هر شغلی نیاز به انجام وظایف به شیوه‌ای حرفه‌ای دارد. برای اینکه یک حرفه در فضای کسب و کار امروز رقابتی بماند، داشتن شایستگی‌ها و قابلیت‌های تخصصی ضروری است. با این حال، غیر از داشتن مهارت‌ها و دانش منحصر به فرد، یک حرفه باید به مجموعه‌ای از اصول اخلاقی نیز پایبند باشد، که هنجارهای خاصی هستند که متخصصان باید از آنها پیروی کنند. کارکنانی که اخلاق حرفه‌ای را رعایت می‌کنند، به مسائل اخلاق در حرفه خود پایبند هستند. هدف منشور اخلاق حفظ سطح بالایی از شایستگی در بین اعضای سازمان، حاکمیت بر تعاملات آنها، ارتقا و حفظ شهرت حرفه و رفاه جامعه حرفه‌ای است. اخلاق حرفه‌ای به دلیل اتکای سازمان به اعتماد ضروری است. اخلاق حرفه‌ای به رفتار افراد در نقش‌های حرفه‌ای مربوط می‌شود که در خدمت اهداف عملی و ایده‌آلیستی قرار می‌گیرند. از این رو، ضروری

است که منشور اخلاقی هم عملی و هم قابل اجرا باشد. پژوهش حاضر با هدف ارائه مدل مدیریت تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای کارکنان در شهرداری‌های کشور انجام گرفت. یافته‌های حاصل از روش تحلیل مضمون حاکی از شناسایی ۲۴۴ مضمون پایه در قالب ۲۴ مضمون سازمان دهنده و ۶ مضمون فراگیر بود.

اولین مضمون فراگیر شناسایی شده اخلاق حرفه‌ای بود. که شامل مؤلفه‌های احترام و کرامت، انصاف و برابری، رعایت ارزش‌های اجتماعی و همدردی و همراهی با دیگران بود. تامین امنیت اطلاعات از جنبه‌های مختلفی تاثیر می‌پذیرد و یکی از جنبه‌های موثر در پیشبرد این هدف، رفتار و اخلاق حرفه‌ای کارکنان است. از این رو دومین مضمون فراگیر عملکرد منابع انسانی است که مولفه‌هایی مانند رفتار فردی، رفتار سازمانی را شامل است. مدیریت عملکرد بیان می‌کند که به منظور حفاظت از داده‌ها، پایش (نظارت) مدیریت از ارکان مؤثر و اساسی است. زمانی که عملکرد افراد و سازمان توسط یک مدیریت منظم و پایبند به اصول اخلاقی، نظارت می‌شود، احتمال بروز رفتارهای غیراخلاقی و ایجاد اختلال در امینت فناوری اطلاعات کاهش می‌یابد. سومین مضمون فراگیر تعهد و مسئولیت پذیری است که دربرگیرنده دو مولفه پاسخگویی و وفاداری است. در هر سازمانی کارکنان میزانی از اطلاعات سازمان را در اختیار دارند با سطوح مختلفی از طبقه بندی، لذا افراد بایستی متعهد به حفظ و نگهداری از این اطلاعات باشند و نسبت به استفاده صحیح و مناسب آن در جهت اهداف سازمان مسئول باشند و در این خصوص پاسخگو باشند. چهارمین مضمون فراگیر شناسایی شده، مدیریت منابع انسانی است. رعایت اخلاق حرفه‌ای در هر حوزه‌ای مستلزم آموزش و نهادینه سازی اصول و ارزشهای حاکم بر آن نزد کارکنان است. عوامل متعددی در این زمینه تاثیرگذار هستند که در این تحقیق برای این مضمون مولفه‌هایی همچون آموزش، توانمندسازی کارکنان، انگیزش، مشارکت و ... شناسایی شد. در نهایت ششمین مضمون فراگیر یکی از مهمترین مضامین شناسایی شده است که ساختار سازمانی نام گذاری شده است. بی شک هم در پیاده سازی خط‌مشی‌های اخلاق حرفه‌ای و هم در استقرار نظام مدیریت امنیت اطلاعات، ساختار سازمانی نقش بسیاربالایی دارد. برای این مضمون مولفه‌های مانند رسمیت، پیچیدگی، اهداف و استراتژی، قوانین و مقررات، مدیریت اطلاعات، ارتباطات و حفاظت و پشتیبانی از اطلاعات شناسایی شد. حفاظت از اطلاعات سازمانی نیازمند یک مدیریت مصمم و پیگیر است و نظارت صحیح می‌تواند جنبه‌های غیراخلاقی احتمالی را کنترل نماید و به تأمین امنیت فناوری اطلاعات کمک کند. رفتار اخلاقی کارکنان در زمینه امنیت فناوری اطلاعات از اهمیت زیادی برخوردار است. اگر کارکنان از خط‌مشی‌ها و اصول اخلاقی پیروی نکنند، ممکن است به نقض امنیت داده‌ها یا سیستم‌ها منجر شود.

پایش و نظارت رفتارها می‌تواند خط‌مشی کارکنان را به آن‌ها یادآوری کند و آن‌ها را در مسیر صحیح رفتاری قرار دهد.

به محققان آینده پیشنهاد می‌شود که میزان صحت و سقم مدل پژوهش را از طریق بررسی‌های میدانی مورد مطالعه قرار دهند. همچنین پیشنهاد می‌گردد که برای دستیابی به پیش‌زمینه‌های شکل‌گیری تأمین امنیت فناوری اطلاعات مبتنی بر خط‌مشی‌های اخلاق حرفه‌ای کارکنان از مصاحبه‌های نیمه ساختاریافته با افراد خبره نیز بهره ببرند. از آنجایی که این مصاحبه‌ها در حین انجام وظایف به کارشناسان کل شهرداری‌های کشور داده شده است، بنابراین شرایط محیطی بر نحوه پاسخگویی آنها بی‌تأثیر نبوده است.

## منابع


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

جعفری، سیدمحمدباقر، و شمسی، فاطمه. (۱۳۹۵). بررسی عوامل اثرگذار بر رعایت اخلاق فناوری اطلاعات. *چشم انداز مدیریت دولتی*، ۲(۲۸ )، ۶۹-۸۷.

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)، ۱-۱۵.

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.

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.

دوستی، مهدی.(۱۴۰۲). اخلاق حرفه‌ای در فناوری اطلاعات. *مهندسی مدیریت*، ۱۶(۸۵)، ۲۰-۱.

رضایی، علی؛ مصدق، محمد جواد و رضایی، مونا.(۱۳۹۷). عوامل اثرگذار بر اثر بخشی نظام مدیریت امنیت اطلاعات. *مجله مدیریت توسعه و تحول*، ۹۷ (۳۳)، ۸۲- ۷۳.

رضوانی، شهلا.(۱۳۹۷). طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی. *پژوهشنامه کتابداری واطلاع‌رسانی*، ۸(۱)، ۳۵۶-۳۳۷.

رئیسی، علیرضا و کریمیان کاکلکی، زهره.(۱۴۰۰). بررسی ارتباط اخلاق حرفه‌ای و ارزش‌های شغلی با رفتارهای انحرافی سازمانی در کارکنان شبکه بهداشت و درمان شهرستان اردل. *مجله دانشگاه علوم پزشکی جیرفت*، ۸(۳)، ۲۰-۱.

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

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

شفیع پور، سیده فاطمه؛ زارع زیدی، علیرضا و متانی، مهرداد.(۱۳۹۶). نقش اخلاق حرفه‌ای مدیران در موفقیت سازمان‌ها. *دو ماهنامه مطالعات کاربردی در علوم مدیریت و توسعه*، ۲(۵)، ۲۰-۱.

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.

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

قربان زاده، پرویز، پیروتی، شادی، قاسمی، حسن و عباس زاده آذر، احد. (۱۳۹۶). مطالعه تطبیقی استانداردهای مهم سیستم مدیریت امنیت اطلاعات )، *کنفرانس ملی فناوریهای نوین در مهندسی برق و کامپیوتر*(ISMS)، اصفهان:موسسه آموزش عالی جهاد دانشگاهی.

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.

ملکی نیا، محمد و موسوی قیداری، سید علیرضا.(۱۴۰۰). اثر امنیت داده‌ها برعملکرد فناوری اطلاعات در محاسبات رایانش ابری. *اولین همایش بین‌المللی جهش علوم مدیریت، اقتصاد و حسابداری*، ساری.

وظیفه، زهرا؛ مهدی، محمد و وکیلی، نادیا.(۱۳۹۷). الگوی امکان‌سنجی و استقرار اثربخش سیستم مدیریت امنیت اطلاعات بر مبنای روش فراترکیب. *فصلنامه علمی-پژوهشی مطالعات مدیریت کسب و کار هوشمند*، ۷(۲۶)، ۹۹-۷۱.

Aggarwal, A. and Ram Kumar, D.(2022). Association between stress and information security policy non-compliance behavior: A meta-analysis. *Computers & Security28 October 2022*.

Akinsanya, M. O., Ekechi, C. C., and Okeke, C. D.(2023). Virtual private networks (vpn): a conceptual review of security protocols and their application in modern networks. *Engineering Science & Technology Journal*, 5(4), 1452-1472.

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

Allahrakha, N.(2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. *Legal Issues in the Digital Age*, 4(2), 78-121.

Andita, R.; and Aditya, F.(2023). Systematic literature review on information security risk management in public service organizations. *Jurnal Teknik Informatika (Jutif)*, 5(1), 89-96.

Buljan, A. and Spremic, M.(2019). Cluster Analysis of IT Security Risks in Chosen Sectors, entrenova Conference Proceedings, *Available at SSRN: https://ssrn.com/abstract=3492251 (http://dx.doi.org/10.2139/ssrn.3492251)*.

Carauleanu, A., Tanasa, I. A., Nemescu, D., & Socolov, D. (2021). Professional ethics, VBAC and COVID-19 pandemic: A challenge to be resolved. *Experimental and Therapeutic Medicine*, 22(3), 1-6.

Chau, J. (2005). Skimming the technical and legal aspects of BS7799 can give a false sense of security. *Computer Fraud & Security*, 9: 8-10.

De Zoysa, A. H. N.(2022). Inculcating Professional Ethics among Employees in the Workplace A Systematic Literature Review. *International Journal of Multidisciplinary Studies (IJMS)*, 9(1):21-34.

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

Emmett, S.(2015). *Excellence in Warehouse Management. Haw to minimize costs and maximize value: TJ*, International Ltd, Paststow, Cornwall, UK.

Finuras, P.(2022). Some Issues Regarding the Ethics of the Management at Romanian State-Owned Companies. *Journal of Intercultural Management and Ethics,* 4(4), DOI: https://doi.org/10.35478/jime.2021.4.06.

Hilhorst, C., et al.(2022). Efficiency gains in public service delivery through information technology in municipalities. *Government Information Quarterly*, 39(2),101724.

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

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

Mivald, A. (2004). *Computer network security*, Translated by Seyyed Ahmad Safai, The first edition, Daneshparvar, Tehran

Nikrerk, J.F. and Van, s.(2017). Information security culture: a management perspective. Computer & security, 5, 142-144.

Paul, P. and Aithal, P. S.(2019). Network Security: Threat & Management, Proceedings of International Conference on Emerging Trends in Management. IT and Education, 1(1), 85-98.

Razikin, K. and Benfano, S.(2022). *Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework*. Egyptian Informatics

Riabova, A., Pogodin, S., Lubina, D., & Sablina, M. (2021, October). *Professional Ethics in Higher Education. In International Conference on Topical Issues of International Political Geography* (pp. 159-170). Cham: Springer International Publishing.

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

Semlambo, A.; Adam, M. G.; Catherine, E. and Wazoel, L.(2021). Factors Affecting the Security of Information Systems: A Literature Review. *The International Journal of Engineering and Science (IJES),* 10(1), 57-65.

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.

Vimercati, S., Foresti, S., Livraga, G. and Samarati, P.(2022). Chapter 18 - Digital infrastructure policies for data security and privacy in smart cities, ELSEVIER: *Smart Cities Policies and Financing Approaches and Solutions*, Pages 249-261, https://doi.org/10.1016/B978-0-12-819130-9.00007-3.

Yazdanmehr, A.; Jawad, M.; Benbunan-Fich, R. and Wang, J.(2023). The role of ethical climates in employee information security policy violations. Decision Support Systems, 177, 114086.