

ETHICAL GOVERNANCE IN THE TRANSFORMATION OF DIGITAL PUBLIC SERVICES AT THE POPULATION AND CIVIL REGISTRATION OFFICE OF SUMEDANG REGENCY

Dewi Maharani ^{a*)}, Dhesti Widya Nurhasanah Ningrum ^{a)}, Fepi Febianti ^{a)},
Arip Rahman Sudrajat ^{a)}

^{a)} Universitas Sebelas April, Sumedang, Indonesia

*Corresponding Author: dewi_maharani_fisip@unsap.ac.id

Article history: received 12 June 2026; revised 26 June 2026; accepted 28 July 2026

DOI: <https://doi.org/10.33751/jhss.v10i02..298>

ABSTRACT. Digital public service transformation requires not only greater efficiency and service accessibility but also governance that ensures integrity, fairness, transparency, accountability, and the protection of citizens' data. This study aims to analyze the implementation of ethical governance in digital public service transformation at the Population and Civil Registration Office of Sumedang Regency. The study employed a qualitative approach with a single-case study design. Data were collected through non-participant observation, documentation, and semi-structured interviews with purposively selected informants representing organizational leaders, division heads, service officers, system operators, and citizens using digital services. The study focused on ethical leadership, ethical standards and codes, ethical organizational culture, accountability and controlling, and ethics education and communication. Data were analyzed using an interactive model comprising data reduction, data display, conclusion drawing, and verification, while data validity was maintained through source and technique triangulation. The findings indicate that ethical governance has been supported by leadership role modelling, standard operating procedures and ethical codes, access restrictions, individual user accounts, multi-level verification, a culture of integrity, system activity records, hierarchical controlling, and employee development. However, its implementation has not been fully optimal due to inconsistent complaint follow-up, reactive use of audit trails, irregular security audits, insufficient protection for internal reporters, the absence of specific and periodic digital ethics training, and limited transparency and clarity in communicating data protection and service status. The study concludes that ethical governance has been institutionalized in internal policies and practices, but further strengthening is required to ensure that its outcomes are consistently experienced by citizens through secure, responsive, transparent, inclusive, and public-oriented digital services.

Keywords: Administrative Ethics; Ethical Governance; Public Service Management; Public Service Transformation; Digitalization of Public Services.

1. INTRODUCTION

Public service is one of the fundamental functions of government that reflects the state's role in fulfilling the basic rights and needs of the people. The quality of public service is not only determined by the speed of service delivery, but also by ease of access, procedural certainty, transparency, accountability, fairness, and the responsiveness of government officials to the needs of the public. Public service thus has both administrative and ethical dimensions, as every action taken by government officials involves the exercise of public authority and the fulfillment of citizens' rights. Kurniawan et al. [1] explain that integrity, responsiveness, fairness, transparency, accountability, and public participation are essential elements in achieving high-quality public services. Therefore, the delivery of public services must not only meet formal requirements but must also be oriented toward the public interest, carried out without discrimination, and be accountable.

Advances in information technology have prompted the government to transform its administrative processes and public

services. Government digitization is characterized by the use of information technology, electronic systems, online platforms, data integration, and automation in the execution of governmental functions. These changes aim to improve bureaucratic efficiency, expedite administrative processes, expand access to information, strengthen transparency, and enhance the government's ability to respond to public needs. Nastia [2] explains that the implementation of e-government can improve efficiency, transparency, accountability, public engagement, and government responsiveness. State that the use of digital technology has the potential to increase bureaucratic efficiency, service transparency, and data-driven decision-making.

The digitization of government is a key part of Indonesia's bureaucratic agenda, specifically through the implementation of the Electronic-Based Government System. The government no longer uses technology merely as an administrative tool but has begun to integrate it into the governance framework. The use of digital technology is

transforming how the government manages information, makes decisions, coordinates organizational activities, and interacts with the public. Sasfiani et al. [3] demonstrate that digital technology and artificial intelligence have the potential to foster more inclusive, efficient, and responsive governance. However, their success depends on the readiness of infrastructure, the competence of government officials, data integration, regulatory support, inter-organizational collaboration, and the public's level of digital literacy.

In practice, the transformation of digital public services does not always proceed optimally or evenly. Juwandi et al. [4] found that the digitization of public services has not yet been fully inclusive, particularly for people in rural areas and groups with limited access and digital literacy. Differences in technological proficiency can create a service gap between those who can access digital services and those who still rely on in-person services. Other barriers include infrastructure limitations, low human resource competency, resistance to change, weak system integration, and suboptimal community involvement [2], [5].

Digital transformation also cannot be assessed solely on the basis of technical efficiency. Halim et al. [6] caution that digital services risk being reduced to impersonal data transactions when technology is prioritized over human values. Data-driven technical rationality can sideline moral considerations, while the automation of services has the potential to diminish empathy, fairness, and the accountability of public officials. Dinata [7] explains that the digital transformation of public administration raises ethical issues such as personal data protection, information security, equal access, accountability for digital decisions, changes in organizational culture, and the protection of citizens' rights. Thus, the transformation of digital public services is not merely a technological issue but also concerns how the government upholds ethical values in an evolving service environment.

This issue has become increasingly important in population administration and civil registration services. The Population and Civil Registration Office manages various types of strategic and sensitive personal data, such as the National Identification Number, Family Card, address, family relationships, marital status, and biometric data. The digitization of population administration services offers benefits such as faster processing, easier access, reduced waiting times, improved accuracy, and easier data integration. However, digital data management also presents risks such as unauthorized access, data breaches, misuse of information, data processing errors, and uncertainty regarding which party is responsible in the event of system disruptions or errors. Therefore, the digitization of population administration must be carried out with due regard for the principles of prudence, security, confidentiality, accountability, and the protection of residents' rights.

The Sumedang Regency Population and Civil Registration Office has developed digital-based services as part of its efforts to improve the quality of population administration services. This digitization is evident, among other things, in the use of Digital Population IDs, the provision of information and a complaint channel through the official website, the Fast Child

Identity Acquisition System (SiCeRIA), and the integration of services with the Tahu Sumedang Public Service Portal. The Tahu Sumedang Portal provides access via the website, Android apps, in-person services at the Public Service Mall, and a WhatsApp Bot. Previously, the Sumedang Regency Population and Civil Registration Office also developed the Online Population Services System (SilaSidakep) to facilitate the online submission of population documents. These various innovations demonstrate efforts to improve the accessibility, efficiency, and responsiveness of civil registration services for the public. Information regarding these services can be found on the Tahu Sumedang portal (<https://tahu.sumedangkab.go.id/>).

The existence of digital platforms does not in and of itself guarantee that the transformation of public services has been carried out ethically. Digital civil registration services must be evaluated based on how leadership builds a commitment to data protection, how standards and codes of ethics are applied in the use of systems, how integrity is embedded in the organizational culture, how data access and system errors are monitored, and how public officials receive training on digital ethics. Furthermore, these services must ensure that members of the public with limited access to devices, internet connectivity, digital skills, or those affected by age, disability, or geographic location still receive equal access to services. Thus, the evaluation of service digitization should not be based solely on speed and convenience but also on fairness, security, transparency, accountability, and the protection of the public interest.

In this context, *ethical governance* is a crucial approach to ensuring that digital transformation remains guided by public values. Ethical governance establishes integrity, responsibility, justice, transparency, accountability, and a focus on the public interest as the foundation of governance. Rahmawati & Nowanda [8] explain that ethics reinforces the principles of *good governance* through transparency, accountability, participation, and compliance with the law. Meanwhile, Nggilu & Mokodongan [5] found that civil servants' digital competencies do not necessarily lead to the internalization of service ethics. Technological competencies need to be integrated with ethics, organizational culture, and leadership so that digital transformation remains human-centered.

This study uses Menzel [9] ideas in *Ethics Management for Public Administrators: Building Organizations of Integrity* as its primary theoretical framework. Menzel [9] explains that public organizations with integrity are shaped not only by the individual morality of their officials but also by the organization's ethics management system. Based on this framework, *ethical governance* in this study is operationalized into five dimensions: ethical leadership, ethical standards and codes of conduct, an ethical organizational culture, accountability and controlling, and ethics education and communication. These five dimensions are used to analyze how ethical values and management mechanisms are integrated into the digital public service transformation at the Sumedang Regency Population and Civil Registration Office.

A number of previous studies have examined digital transformation from the perspectives of *e-government*, service innovation, civil servant competencies, the use of artificial

intelligence, and service quality. Other studies have examined service ethics, *good governance*, data privacy, the digital divide, and the risk of service dehumanization. However, these studies tend to treat technological and ethical aspects as separate topics. Furthermore, some studies remain conceptual in nature or focus on agencies that do not specifically manage population data. Empirical studies that analyze the integration of ethical management into the overall process of digital service transformation within population administration agencies at the local government level remain limited.

This study fills that gap by adopting *ethical governance* as the primary perspective for analyzing the transformation of digital public services. The novelty of this study lies in the use of five operationalized dimensions derived from Menzel's framework to analyze not only the ethical behavior of civil servants but also the organizational mechanisms that underpin digital services with integrity. The analysis covers the role of leadership, the existence of ethical standards, the shaping of organizational culture, accountability and controlling mechanisms, as well as education and communication regarding digital ethical risks in civil registration services.

Based on the above discussion, this study aims to analyze *ethical governance* in the digital transformation of public services at the Sumedang Regency Population and Civil Registration Office through the dimensions of ethical leadership, ethical standards and codes of conduct, an ethical organizational culture, accountability and controlling, as well as ethics education and communication. This study is expected to make a theoretical contribution to the development of public administration ethics research in the context of digital transformation, while also providing practical recommendations for strengthening population administration services that are integrity-driven, secure, accountable, inclusive, and community-oriented.

2. METHOD

This study employs a qualitative approach using a single-case study design (*single-case study*). The qualitative approach was chosen because the study aims to gain an in-depth understanding of the application of *ethical governance* in the transformation of digital public services within the context of a specific organization. Qualitative research allows researchers to understand the experiences, perspectives, behaviors, processes, and interactions of the actors involved in the delivery of digital services.

Yin [10] explains that a case study is an empirical research method used to examine a contemporary phenomenon in depth within a real-life context, particularly when the boundary between the phenomenon and its context is not clearly defined. A single-case study design can be used when the research focuses on a single case that possesses specific, critical, representative, or relevant characteristics to comprehensively explain a particular phenomenon. In this study, the single case examined is the implementation of *ethical governance* in the digital transformation of public services at the Population and Civil Registration Office of Sumedang Regency. The Population and Civil Registration Office of Sumedang Regency was selected as the case study unit because the agency provides

digital-based public services while also managing population data that is personal, strategic, and sensitive. These conditions make it essential to conduct an in-depth examination of the dimensions of leadership, ethical standards, organizational culture, accountability, controlling, and ethics education.

The unit of analysis for this study is ethical governance in the process of transforming digital public services at the Sumedang Regency Population and Civil Registration Office. The research focuses not only on the existence of service applications or technologies, but also on how the organization integrates the values of integrity, accountability, data security, fairness, transparency, and public interest orientation into leadership, service procedures, civil servant behavior, controlling systems, and employee competency development.

The research data consists of primary and secondary data. Primary data was obtained directly through observation and interviews with informants involved in policy formulation, system management, service delivery, controlling, and the use of digital public services. Secondary data is obtained from regulations, service standards, standard operating procedures, codes of ethics, performance reports, complaint reports, public satisfaction survey results, information security documents, government publications, and relevant scientific articles.

Data collection was conducted through a literature review and field research. The literature review was used to examine theories, concepts, previous research findings, and policies related to public services, digital transformation, *digital governance*, public administration ethics, data protection, and *ethical governance*. Literature sources included books, journal articles, laws and regulations, government reports, policy documents, and other official sources that are academically credible.

The field study was conducted through observation, documentation, and interviews. According to Sugiyono [11], data collection techniques in qualitative research can be carried out through observation, interviews, documentation, and triangulation. Observations were conducted by directly observing the process of providing civil registration services, the use of digital systems, interactions between officials and the public, assistance provided to service users, the implementation of data security procedures, and the handling of service obstacles. Observations were conducted in a non-participatory manner, meaning that the researcher acted as an observer and was not directly involved in the service process.

Documentation is used to obtain written and visual data related to the research subject. The documents analyzed include regulations, digital service policies, codes of ethics, service announcements, standard operating procedures, service standards, data access authority assignments, performance reports, public satisfaction survey results, complaint data, outreach materials, training materials, evaluation reports, screenshots of service platforms, and other relevant documents. Documentation is used to corroborate, confirm, or compare information obtained through observation and interviews.

The interviews were conducted using a semi-structured approach, following an interview guide developed based on the research focus. Semi-structured interviews allow researchers to ask prepared questions while also exploring additional

information based on the informants' responses and experiences. The interviews were designed to gather information on leadership commitment, the implementation of ethical standards, work culture, data protection, accountability mechanisms, system controlling, public complaints, staff training, and communication regarding digital ethics risks.

Informants were selected using purposive sampling. Sugiyono [11] explains that *purposive sampling* is a technique for selecting data sources based on specific criteria, namely that informants are chosen because they are deemed to have knowledge of, experience with, and involvement in the phenomenon under study. The number of informants is not determined solely by quantity, but by the adequacy and depth of the information. Data collection may be halted when the information has reached saturation or no longer yields new themes.

The informants in this study consisted of:

1. Head of the Population and Civil Registration Office of Sumedang Regency.
2. Head of the Division of Population Administration Information Management and Data Utilization at the Sumedang Regency Population and Civil Registration Office.
3. Head of the Population Registration Services Division, Sumedang Regency Population and Civil Registration Office.
4. Head of the Civil Registration Services Division, Sumedang Regency Population and Civil Registration Office.
5. Population Administration Service Officer at the Sumedang Regency Population and Civil Registration Office.
6. Digital Service System Operator at the Sumedang Regency Population and Civil Registration Office.
7. The public who use digital civil registration services.

The research analysis instruments were developed based on Menzel [9] ideas regarding *ethics management* and the development of organizations with integrity. These concepts were operationalized into the following five research dimensions:

1. Ethical Leadership
2. Standards and Code of Ethics
3. Ethical Organizational Culture
4. Accountability and controlling
5. Ethics Education and Communication

Data analysis was conducted using the Miles and Huberman interactive model, as described by Sugiyono [11]. The stages of analysis included data reduction, data presentation, and drawing conclusions and verification.

Data reduction was conducted by selecting, focusing, simplifying, grouping, and coding the data obtained from interviews, observations, and documentation. The data was grouped based on Menzel's five dimensions: ethical leadership, ethical standards and codes, an ethical organizational culture, accountability and controlling, and ethics education and communication. The researchers also remained open to the possibility of new themes emerging outside the initial framework, particularly those related to accessibility, data protection, the digital divide, and community experiences.

The data is presented in the form of narrative descriptions, thematic matrices, tables comparing informants, interview excerpts, and relationships among findings. This presentation is used to identify patterns, similarities, differences, relationships, and potential discrepancies between formal policies and service practices. Next, conclusions are drawn and verified by interpreting the identified patterns and themes. Initial conclusions are provisional and are continuously verified using additional data, documents, and cross-referencing among sources until consistent and reliable findings are obtained.

Data validity was ensured through source triangulation, methodological triangulation, and cross-checking of information. Source triangulation was conducted by comparing statements from leaders, government officials, system administrators, service staff, and the public. Methodological triangulation was conducted by comparing the results of interviews, observations, and documentation. Whenever inconsistencies in information were found, the researchers sought clarification or collected additional data. The study also adheres to research ethics by clearly stating the research objectives, obtaining informants' consent, protecting informants' identities, maintaining the confidentiality of interview results, and restricting the inclusion of sensitive information regarding the system and population data.

3. RESULTS

Ethical Leadership

Ethical leadership in *ethical governance* is a form of government leadership that prioritizes integrity, fairness, transparency, accountability, compliance with the law, and the public interest as the foundation for decision-making. Ethical leaders are not only required to demonstrate personal moral conduct but are also responsible for fostering an organizational environment that encourages public servants to deliver services in accordance with ethical standards. In the digital transformation of public services, ethical leadership ensures that the use of technology is directed not only toward improving speed and efficiency but also toward protecting citizens' rights, preventing abuse of authority, safeguarding data security, and maintaining service accountability. Bian & Wang [12] explain that ethical leadership in digital government transformation plays a role in guiding civil servants' behavior, strengthening motivation for public service, and ensuring that government innovation remains focused on creating public value.

From a public administration perspective, ethical leadership does not stop at the character of individual leaders, but must be institutionalized through organizational policies, service standards, standard operating procedures (SOPs), codes of ethics, the delegation of authority, controlling, complaint mechanisms, and controls on data usage. Leaders serve as both moral guides and ethical stewards who communicate organizational values, set an example, oversee the conduct of public officials, provide protection to employees who uphold integrity, and take corrective action when violations occur. Pakhnenko & Kuan [13] categorize ethical issues in digital governance into three aspects: privacy, security, and data protection; transparency and accountability; and inclusion,

accessibility, and nondiscrimination. Thus, ethical leadership in digital public services can be assessed based on leaders' ability to balance efficiency, data security, equitable access, responsiveness, and the protection of citizens' rights.

Ethical leadership at the Sumedang Regency Population and Civil Registration Office has been evident in the organization's commitment to integrity, fairness, transparency, data protection, document accuracy, and the fulfillment of citizens' rights. This commitment has been implemented through standard operating procedures (SOPs), data access restrictions, document verification, public assistance, and the management of risks associated with digital services. However, its implementation has not yet been fully optimal because the public still experiences delays in the follow-up to complaints, assistance from staff that is not always prompt, digital procedures that are not yet easy to understand, and unequal access for groups with limited digital literacy. These conditions indicate that ethical values have evolved at the policy level and within the organization, but the results are not always consistently felt by all service users. Juwandi et al. [4] explain that the transformation of digital public services must integrate the values of justice, humanity, protection of individual rights, and nondiscrimination so that technological innovations do not create new service disparities.

The Head of the Sumedang Regency Population and Civil Registration Office explained that digital transformation is not only intended to expedite services but also to ensure that services are conducted with integrity, fairness, transparency, security, and a focus on the public's interests. These values are embodied through service standards, standard operating procedures (SOPs), a code of ethics, the delegation of authority, data access restrictions, complaint mechanisms, service evaluations, multi-channel services, assistance, and proactive outreach services. Leadership sets an example by refraining from accessing data outside the scope of official duties, not instructing staff to bypass procedures, and not disclosing data to unauthorized parties. When there is a conflict between service speed and data security, leaders prioritize verification, accuracy, and data protection. From a public administration perspective, these practices demonstrate the role of leaders as both a *moral person* and a *moral manager*—that is, exhibiting ethical behavior and institutionalizing it within the organizational system. Jha & Singh [14] emphasize that ethical leadership fosters an ethical climate through exemplary conduct, communication of values, organizational support, and the reinforcement of behavioral standards that serve as guidelines for employees in performing their duties.

The Head of the Division of Population Administration Information Management and Data Utilization at the Sumedang Regency Population and Civil Registration Office emphasized the responsible use of data. Operators and staff are instructed to access data in accordance with their duties and authorities, use individual accounts, maintain password confidentiality, and refrain from storing or sharing data via unsecured devices and channels. Requests for data utilization from other units or agencies are reviewed based on official mechanisms, legal basis, purpose of use, necessity, proportionality, and the recipient's ability to ensure data security. Reports regarding vulnerabilities

or suspected misuse are addressed through verification, temporary security measures, investigations, the imposition of actions commensurate with the severity of the violation, and system evaluation. These practices of access restriction, data minimization, and activity logging reflect *digital accountability*, as every instance of data use must be traceable and accountable. Pakhnenko & Kuan [13] emphasize that the protection of privacy and data security is a primary ethical responsibility in digital governance because data misuse can harm the public and erode trust in the government.

The Head of the Population Registration Services Division at the Sumedang Regency Population and Civil Registration Office explained that staff are instructed to provide services based on established standards and the order in which applications are received, without discriminating based on personal connections, position, economic status, ethnicity, religion, gender, or social background. The speed of service is still a priority, but it must not compromise the verification process or the accuracy of documents. Members of the public who are unable to use digital procedures are provided with assistance, in-person services, or support through subdistricts, villages, Public Service Centers, and outreach services. In the event of an error in document issuance, officials investigate the source of the error, provide an explanation and correction without causing undue hardship to the public, and implement system improvements or corrective measures. In public administration, these services reflect procedural and distributive justice because citizens not only receive equal treatment but also assistance tailored to their needs. Juwandi et al. [4] emphasize that ethical digital transformation must ensure services that are fair, humane, inclusive, and focused on protecting citizens' rights.

The Head of the Civil Registration Services Division at the Sumedang Regency Population and Civil Registration Office emphasized that services related to birth, death, marriage, and divorce certificates, as well as other civil registration documents, must be provided fairly, transparently, and with a focus on fulfilling the rights of the public. Complex and sensitive cases are handled with due consideration for legality, confidentiality, data accuracy, the dignity of the applicant, and the impact of decisions on relevant parties. Members of the public requiring special assistance receive priority, guidance, direct services, facilitation through village or subdistrict governments, and outreach services. Accuracy is maintained through document verification, tiered reviews, division of tasks, and the use of checklists, ensuring that speed targets do not compromise the validity of documents. These practices demonstrate the application of the principles of prudence and equitable administration, as decisions regarding civil registration services are directly linked to the legal status and civil rights of citizens. Pakhnenko & Kuan [13] explain that digital innovations must be accompanied by accountability, the protection of rights, and risk management to ensure that increased efficiency does not compromise the accuracy and legitimacy of administrative decisions.

Population Administration Service Officers at the Sumedang Regency Population and Civil Registration Office confirmed that management provides guidance on ethics and

integrity through roll calls, internal meetings, evaluations, training, and the dissemination of standard operating procedures (SOPs). Officials are instructed to provide fair and non-discriminatory service, to refuse any form of compensation, to not prioritize applicants based on personal connections, and to use data solely for service purposes. When facing ethical dilemmas, officials are instructed to consult their superiors in a hierarchical manner and to seek support when refusing requests that do not comply with procedures. Staff are also given the opportunity to report system malfunctions, unclear procedures, verification difficulties, and data security risks, although the effectiveness of this process still depends on the consistency of management's follow-up. From the perspective of public organizational behavior, these conditions indicate the formation of an *ethical climate* and *employee voice*, but their sustainability requires a clear response from management to employee reports. Jha & Singh [14] state that ethical leadership can encourage employees to speak up about problems if leaders create a safe climate, value input, and follow up on reported issues.

The Digital Service System Operator at the Sumedang Regency Population and Civil Registration Office explained that use of the system is restricted to official business only and is tailored to each user's authority. Operators are required to use individual accounts, keep their passwords confidential, lock their devices, and refrain from storing or sending public documents via personal devices or channels. Reports regarding disruptions, vulnerabilities, or suspected misuse are addressed through verification, access restrictions, account deactivation, activity log reviews, technical coordination, and system evaluations. Operators also receive support when denying access requests that lack an official purpose, legal basis, supporting documentation, or approval from an authorized official. This demonstrates that ethical leadership is realized not only through instructions but also through the organization's protection of employees who uphold system integrity. Al Halbusi et al. [15] explain that ethical leadership becomes more effective when organizations provide tangible support to employees who uphold ethical standards, including when they face pressure to take actions that violate the rules.

Users of the digital services provided by the Sumedang Regency Population and Civil Registration Office believe that these digital services have helped save time and travel costs, as well as reduced the need to visit service offices in person. Officials have also provided assistance and addressed public complaints. However, the benefits of these services have not been felt equally, as those with devices, internet access, and digital literacy enjoy greater convenience compared to the elderly, people with disabilities, low-income individuals, rural residents, and groups with limited digital access. Assistance from staff is not always readily available during peak service hours, while follow-ups on complaints are not always accompanied by updates on progress or a confirmed resolution timeline. From a public administration perspective, this situation highlights a gap between *administrative intention* and *citizen experience*—that is, the discrepancy between an organization's internal commitments and the services actually experienced by the public. Ciesielska et al. [16] explain that digital exclusion is influenced by social and technical factors, such as age, ability,

economic status, access to technology, digital skills, and the suitability of systems to user needs.

There is alignment between the commitments made by the Head of the Sumedang Regency Population and Civil Registration Office and their implementation by the Head of the Division of Population Administration Information Management and Data Utilization, the Head of the Division of Population Registration Services, the Head of the Division of Civil Registration Services, Population Administration Service Officers, and Digital Service System Operators. This alignment is evident in four key aspects: compliance with standard operating procedures (SOPs), data access restrictions, a balance between speed and security, and attention to groups with limited digital access. This demonstrates that ethical leadership does not stop at normative statements but has been translated into practices such as access management, document verification, community assistance, and risk management. Bian & Wang [12] emphasize that ethical leadership can drive digital government transformation when leaders' values are supported by organizational capacity, internal communication, knowledge management, and the readiness of civil servants to translate these values into service practices.

Although there is alignment at the internal level, the experiences of Digital Service Users indicate that the benefits of ethical leadership have not yet been consistently realized. Internal informants described the availability of inclusive service policies, assistance, complaint channels, data access restrictions, and follow-up mechanisms, whereas the public still encounters delays in responses, a lack of clarity regarding the status of complaints, digital instructions that are not yet easy to understand, and disparities in the benefits of services. These gaps indicate that internal accountability has not yet fully transformed into public accountability oriented toward the public's experience. Nurlinah et al. [17] found that digital transformation can increase public trust in the government, but its impact is not always uniform because it is influenced by differences in infrastructure, digital literacy, and the quality of service experiences between urban, semi-urban, and rural areas.

Ethical leadership at the Sumedang Regency Population and Civil Registration Office has thus been institutionalized at the levels of values, policies, organizational controls, and civil servant behavior, but has not yet been fully realized at the level of public experience. Leaders have fulfilled their roles as providers of moral guidance, role models, controllers of data access, guardians of document accuracy, and protectors of staff who adhere to procedures. However, improvements are still needed in the consistency of complaint follow-up, the speed of assistance provision, the simplicity of digital instructions, the certainty of completion timelines, and the equitable distribution of alternative services. Pakhnenko & Kuan [13] emphasize that the ethics of digital governance must integrate data protection, transparency and accountability, as well as inclusion and nondiscrimination. Therefore, new ethical leadership can only be considered optimal if the commitments implemented within the organization are consistently experienced by the public through services that are secure, fair, responsive, transparent, and inclusive.

Standards and Code of Ethics

Standards and codes of ethics in *ethical governance* constitute a set of values, principles, rules of conduct, and operational procedures that guide public officials in exercising their authority and providing services to the public. Service standards establish requirements, procedures, completion times, costs, service outcomes, and complaint mechanisms, while codes of ethics govern the moral obligations of public officials, such as integrity, objectivity, fairness, confidentiality, professionalism, and the prohibition against the abuse of authority. In public administration, both serve as control mechanisms to ensure that civil servants' actions not only comply with legal provisions but also align with the values of the public interest. Ahmad et al. [18] explain that the ethical behavior of civil servants is influenced by leadership, organizational culture, professionalism, ethics education, and the existence of systems capable of preventing and addressing unethical behavior.

In the transformation of digital public services, standards and codes of ethics also encompass rules governing the collection, processing, storage, use, exchange, and security of public data. These standards are necessary to determine who can access the data, the purposes for which the data may be used, the limits of user authority, permitted devices, mechanisms for logging activities, and procedures for handling security incidents. Pullen et al. [19] emphasize that digital ethics must be institutionalized through structural, procedural, and relational mechanisms so that ethical principles do not remain merely normative commitments. Thus, standards and codes of ethics in digital services must be able to integrate legal provisions, public service values, technical procedures, and civil servant accountability.

Standards and codes of ethics at the Sumedang Regency Population and Civil Registration Office have generally been implemented quite well. Digital services are supported by laws and regulations, policies from the Ministry of Home Affairs, service standards, standard operating procedures (SOPs), service announcements, civil service codes of ethics, and integrity pacts. These instruments regulate services that are fast, easy, free, transparent, accountable, and non-discriminatory, while also ensuring the confidentiality of population data. However, there are still issues that have not been regulated in detail, particularly the management of digital security risks, the provision of information regarding data usage, the resolution of non-routine service situations, and incident response procedures. This situation indicates that the existence of formal standards does not automatically guarantee optimal *ethical governance* if it is not accompanied by updates, outreach, controlling, and consistent enforcement. Khamzina et al. [20] emphasize that institutionalizing integrity in the public sector requires integration among ethical regulations, organizational culture, controlling mechanisms, and the enforcement of behavioral standards.

The Head of the Sumedang Regency Population and Civil Registration Office explained that the implementation of digital services has been guided by laws and regulations, policies from the Ministry of Home Affairs, service standards, standard operating procedures (SOPs), service announcements, the civil

service code of ethics, and the integrity pact. These standards emphasize services that are fast, easy, free, transparent, accountable, non-discriminatory, and guarantee the confidentiality of population data. Access rights to data are restricted based on duties, positions, authority, and service needs. From a public administration perspective, the existence of these instruments demonstrates the institutionalization of ethics, as service values are translated into rules and limits on authority that are binding on civil servants. However, the effectiveness of a code of ethics is determined not only by the completeness of the document but also by the internalization of values, leadership by example, controlling, and consistency in its application. Ahmad et al. [18] assert that a code of ethics will influence civil servants' behavior if it is supported by ethical leadership, a culture of integrity, professionalism, and mechanisms to prevent violations.

The Head of the Division of Population Administration Information Management and Data Utilization at the Sumedang Regency Population and Civil Registration Office stated that data management standards cover the collection, processing, storage, utilization, and sharing of population data. Each user is granted access rights according to their role, uses an individual account, and their activities can be traced through an *audit trail*. The use of personal devices, unofficial networks, personal accounts, and external storage media is restricted due to the potential for data leaks and misuse. Although these standards have provided a foundation for security, the evolution of threats such as *phishing*, identity theft, *malware*, social engineering, and account takeovers demands continuous updates to the standards. This indicates that digital ethics standards must be adaptive to changing risks, rather than relying solely on compliance with static procedures. Pakhnenko & Kuan [13] identify privacy, security, and data protection as the primary concerns of digital governance ethics, which require access restrictions, usage controls, and accountability at every stage of data processing.

The Head of the Population Registration Services Division at the Sumedang Regency Population and Civil Registration Office explained that digital services for the electronic ID card (KTP-el), Family Card (Kartu Keluarga), Child Identity Card (Kartu Identitas Anak), population transfers, and data element changes have been implemented in accordance with the standard operating procedures (SOPs) for each type of service. The SOPs govern the receipt of applications, the review of requirements, data verification and validation, processing through the Population Administration Information System, official approval, document issuance, and the delivery of results. Requirements, procedures, processing times, fees, and service status have been communicated through various channels; however, information regarding application stages, reasons for document rejection, and service status updates still needs to be made simpler and more detailed. In public administration, this situation demonstrates that transparency depends not only on the availability of information but also on the public's ability to understand and utilize that information. [21] explains that the public's assessment of the effectiveness of e-services is influenced by their ability to understand and use digital information. Therefore, service information standards must be

formulated in language that is simple, specific, and easily accessible to users with varying levels of digital literacy.

The Head of the Civil Registration Services Division at the Sumedang Regency Population and Civil Registration Office explained that services for birth, death, marriage, and divorce certificates, as well as other civil registration documents, are governed by standard operating procedures (SOPs) tailored to the characteristics of each significant event. These standards require verification of identity, the validity of documents, the consistency of data within the Population Administration Information System, and the legal basis for registration. Stricter safeguards are applied to documents containing sensitive information regarding personal and family circumstances. Applications are put on hold for further clarification and review if documents are incomplete, inconsistent, or suspected of being invalid. These measures reflect the principles of prudence and administrative accountability, as civil registration documents are directly linked to citizens' legal status and civil rights. Pakhnenko & Kuan [13] explain that data security, accountability, and the protection of rights must be integrated into digital service standards so that technological efficiency does not undermine the validity and legitimacy of administrative decisions.

An official from the Population Administration Services Division at the Sumedang Regency Population and Civil Registration Office stated that the Standard Operating Procedures (SOPs) and code of ethics provide sufficiently clear guidelines for the delivery of routine services. Officials are required to be courteous, fair, and transparent; not to solicit bribes; to maintain data confidentiality; and not to impose requirements beyond established regulations. However, there are still situations that have not been addressed in detail, such as ambiguous digital documents, applications submitted by representatives, data discrepancies between agencies, suspected unauthorized use of identity, and urgent service requests when the system is down. These issues are typically resolved through consultation with superiors and the application of the principle of prudence. This situation demonstrates that SOPs have helped standardize services but have not fully anticipated the dilemmas arising from the complexity of digital services. Pullen et al. [19] emphasize that digital ethics governance cannot rely solely on written rules but also requires mechanisms for consultation, deliberation, and decision-making that help public officials resolve ethical issues in situations not explicitly covered by procedures.

Digital Service System Operators at the Sumedang Regency Population and Civil Registration Office emphasize that system operations adhere to the Standard Operating Procedures (SOPs) for the Population Administration Information System, including data verification and validation, access rights management, document issuance, and incident handling. Each operator uses an individual account, maintains password confidentiality, uses official devices, and refuses access requests outside the scope of their duties. In the event of a system error or suspected data breach, operators are required to secure access and devices, preserve digital evidence, and report the incident to administrators and management. However, incident response procedures still need to be developed in

greater detail and supported by periodic simulations. These conditions indicate that basic security measures are in place, but the organization's digital resilience requires clearly defined roles, reporting channels, recovery steps, incident documentation, and evaluation processes. Figueroa et al. [22] explain that e-government security requires an integrated approach that combines risk management, secure data exchange, cybersecurity governance, and continuous organizational capacity building.

Users of the digital services provided by the Sumedang Regency Population and Civil Registration Office reported that information regarding requirements, procedures, fees, and types of services is generally available. Population administration services are provided free of charge, and the documents requested generally align with the needs of the service. However, the public has not yet received detailed information regarding the purpose of data use, the parties authorized to access the data, the methods and duration of data storage, and the procedures to follow in the event of misuse. Explanations regarding the reasons for document rejection or correction, as well as complaint channels, are also not always provided in a specific manner. From the perspective of *citizen-centered public administration*, data transparency is not sufficiently achieved merely through the availability of a privacy policy; rather, it must provide the public with understanding and control over their personal data. Pakhnenko & Kuan [13] emphasize that transparency, accountability, privacy, and security are interrelated dimensions in building trust in digital government.

There is consistency regarding the existence of SOPs for each type of service, access restrictions, the use of individual accounts, multi-layered verification, the protection of sensitive documents, and the prohibition on using data for non-official purposes. This indicates that standards and codes of ethics have been institutionalized within the structure and processes of public services. Ahmad et al. [18] explain that strengthening public sector integrity requires a comprehensive approach that integrates ethical guidelines, leadership, professionalism, organizational culture, education, and the prevention of misconduct.

Although the regulatory and operational framework is in place, there remains a gap between the comprehensiveness of internal standards and the understanding of the public who use digital services. Internal standards have regulated authority, access rights, verification, account usage, and document protection, but the public has not yet received adequate information regarding the purposes of data processing, who can access the data, retention periods, the status of requests, reasons for the return of files, and mechanisms for addressing data misuse. These conditions indicate that standards and codes of ethics have not yet been fully translated into public transparency. Lee-Geiller [21] emphasizes that the effectiveness of e-services and trust in the government are influenced by the quality of the user experience as well as the public's ability to understand digital information. Therefore, the communication of service standards must take into account the simplicity of language, the level of detail in the information, accessibility, and variations in the public's digital literacy.

The standards and code of ethics governing the digital transformation of public services at the Sumedang Regency Population and Civil Registration Office have a sufficiently strong regulatory and operational foundation, but they are not yet fully optimized. The strengths in this area are evident in the existence of standard operating procedures (SOPs) for each service, access restrictions, the use of individual accounts, *audit trails*, multi-layered verification, protection of sensitive documents, and a prohibition on the use of data for non-official purposes. Meanwhile, weaknesses lie in the lack of detailed guidelines for resolving digital ethical dilemmas, incident response procedures, updates to standards for addressing cyber threats, and the dissemination of data protection information to the public. Pullen et al. [19] emphasize that digital ethics governance requires the integration of structural, procedural, and relational mechanisms. Therefore, optimizing this dimension requires periodic updates to standard operating procedures (SOPs), technical guidelines for resolving digital ethics issues, incident response simulations, enhanced civil servant competencies, and the communication of information regarding services and data protection in a manner that is clearer, simpler, more transparent, and easier for the public to understand.

Ethical Organizational Culture

An ethical organizational culture in *ethical governance* is a system of shared values, norms, beliefs, and practices that shapes public officials' understanding of what constitutes appropriate and inappropriate behavior in the performance of their governmental duties. An ethical culture is reflected not only in the existence of a code of ethics and formal rules, but also in the way leaders set an example, employees make decisions, the organization responds to mistakes, and members of the organization remind one another when they encounter actions that potentially violate public service values. Roy et al. [23] explain that an ethical organizational culture is a component of organizational culture that reflects shared values, norms, and beliefs regarding appropriate behavior and influences the ethical decision-making and actions of organizational members.

In the transformation of digital public services, an ethical organizational culture has a broader scope because it encompasses the values of integrity, professionalism, fairness, empathy, service orientation, and responsibility for data security. An ethical culture is formed when public officials safeguard data not merely out of fear of sanctions, but because they understand that such data relates to the privacy, rights, and interests of the public. This culture also requires a balance between the goal of service speed and the obligation to ensure accuracy, security, and the quality of interactions with users. Pullen et al. [19] emphasize that digital ethics must be institutionalized through structural, procedural, and relational mechanisms so that ethical considerations become part of daily work practices, rather than merely administrative compliance.

An ethical organizational culture at the Sumedang Regency Population and Civil Registration Office has developed through leadership by example, the implementation of a code of ethics and a code of conduct for civil servants, the signing of integrity pacts, regular briefings, controlling, and the practice of

mutual monitoring and reminders. Values such as integrity, professionalism, honesty, responsibility, prudence, fairness, data confidentiality, and a service-oriented mindset have been reflected in the delivery of services. However, the internalization of these values has not been entirely uniform, as some ethical behaviors still depend on supervision and reminders. Workload, limited human resources, pressure to meet targets, system disruptions, and concerns about reporting violations also affect the consistency of ethical value implementation. Roy et al. [23] explain that the strength of an ethical culture is determined by the clarity of values, leadership by example, openness to discussing ethical issues, support for ethical behavior, and consistency in enforcing rules.

The Head of the Sumedang Regency Population and Civil Registration Office explained that an ethical organizational culture is built through leadership by example, the implementation of codes of ethics and codes of conduct for civil servants, integrity pacts, regular briefings, and controlling of service delivery. The values emphasized include integrity, professionalism, honesty, responsibility, prudence, fairness, confidentiality, and a service-oriented approach. The success of services is not only assessed by the number and speed of document processing but also by the accuracy of data, the protection of citizens' rights, courtesy, and civil servants' compliance in exercising their authority. These conditions indicate that performance metrics are beginning to integrate both the technical and ethical dimensions of service delivery. Van der Wal & Demircioglu [24] explain that an ethical culture and ethical leadership can align with public sector innovation when the value of integrity is integrated into organizational processes, rather than being viewed as an obstacle to change and performance achievement.

The Head of the Division of Population Administration Information Management and Data Utilization at the Sumedang Regency Population and Civil Registration Office stated that employees and operators generally understand their obligation to maintain the confidentiality of population data. This awareness is evident in the use of accounts according to assigned duties, restrictions on document access, verification of applicant identities, and consultation with supervisors when there are questionable data requests. However, actions such as changing passwords, locking devices when left unattended, deleting temporary documents, and using official communication channels are not always carried out consistently without supervision or reminders. This situation indicates that the data security culture is still transitioning from formal compliance toward ethical internalization. Magnusson et al. [25] emphasize that information security in the public sector cannot be treated solely as a technical issue but must be an organizational process encompassing leadership, employee awareness, training, controls, accountability, monitoring, and continuous learning.

The Head of the Population Registration Services Division at the Sumedang Regency Population and Civil Registration Office explained that integrity, honesty, responsibility, and empathy are demonstrated through services provided in accordance with standard operating procedures (SOPs), a prohibition on soliciting bribes, non-discriminatory treatment, thorough document verification, and the provision of

assistance to members of the public facing difficulties. Staff are instructed to accept complaints openly and not to be defensive when service errors are identified. However, the high volume of requests and limited staff can lead to more brief communication and increase the risk of reduced accuracy. These findings reveal a potential conflict between a focus on productivity and the ethical quality of service. Roy et al. [23] explain that an ethical culture requires organizational conditions that enable employees to put ethical values into practice. When workloads and performance demands are unrealistic, employees may face pressure to disregard ethical considerations in order to meet operational targets.

The Head of the Civil Registration Services Division at the Sumedang Regency Population and Civil Registration Office emphasized that an ethical organizational culture is crucial because civil registration services deal with sensitive personal and family information, such as births, deaths, marriages, divorces, child acknowledgment, and child adoption. Officials are required to demonstrate empathy, maintain confidentiality, use non-judgmental language, and serve the entire community fairly. A culture of mutual accountability is enforced through document reviews prior to issuance and reprimands when documents are left behind, devices are left unlocked, or sensitive information is discussed in public spaces. This demonstrates the development of informal social control that complements the organization's formal controlling. Al Halbusi et al. (2021) explain that an ethical climate and culture can foster ethical behavior among employees when organizational values are translated into habits, exemplary conduct, controlling, and mutual support among members.

Population Administration Service Officers at the Sumedang Regency Population and Civil Registration Office stated that the values of honesty, responsibility, empathy, and fairness have been applied in their daily work. The officers strive to convey the actual status of services, assist members of the public who are not tech-savvy, safeguard documents, and report and correct errors. The officers also have a practice of cross-checking and reminding one another. However, the officers do not yet feel entirely safe reporting suspected violations involving coworkers or superiors, as they worry about disrupting work relationships or being perceived as blaming others. This situation indicates that an ethical culture is not yet fully supported by psychological safety. Potipiroon & Wongpreedee [26] found that the relationship between the ethical climate and local government employees' willingness to report violations is mediated by psychological safety. Employees are more likely to report violations when the organization provides safe channels and protects whistleblowers from negative consequences.

Digital Service System operators at the Sumedang Regency Population and Civil Registration Office recognize that safeguarding data security is not merely an administrative obligation but also a moral responsibility to the public. The operators understand that having access rights does not grant them the freedom to access or use data beyond the scope of service delivery. Nevertheless, work pressure, a limited number of operators, network disruptions, and demands to complete services can create risks of unsafe work practices, such as borrowing accounts, sharing devices, transferring documents, or

skipping verification steps. Although such actions are prohibited, the potential for their occurrence indicates that ethical behavior is also influenced by the alignment between job demands and organizational resources. Magnusson et al. [25] explain that information security governance in the public sector requires clear responsibilities, employee awareness, adequate resources, access controls, training, monitoring, and management support so that security compliance can be consistently enforced.

Users of the Sumedang Regency Population and Civil Registration Office's digital services generally find the staff to be friendly, honest, helpful, responsive, careful, and non-discriminatory. Digital services also offer convenience by reducing the need for people to visit the office and wait in line. However, the quality of explanations is not always consistent across staff members. When lines grow longer, staff responses tend to be briefer, whereas users who are less tech-savvy require more time and assistance. This can create the impression of unequal service, even though it is not intentional discrimination. Digital services can also feel impersonal if the public receives only automated notifications without explanations or opportunities for consultation. Lee-Geiller [21] emphasizes that assessments of the effectiveness of electronic services are influenced by digital literacy and user experience. Therefore, digitization still requires human support to ensure that services are understood, trusted, and accessed equitably by the public.

The public's assessment of friendliness, honesty, diligence, and helpfulness further reinforces the alignment with the values that shape the organizational culture at the Sumedang Regency Population and Civil Registration Office. Roy et al. [23] explain that an ethical organizational culture is formed when formal values, leadership behavior, work practices, and norms among employees reinforce one another and provide a consistent understanding of the behavior expected by the organization.

Although ethical values have evolved, their internalization has not been entirely uniform or consistent, particularly when organizations face service pressures. The reliance on reminders for safety procedures, variations in communication quality, high workloads, limitations in staff and equipment, the potential for informal work practices, and concerns about reporting violations all indicate a gap between stated values and actual work practices. These conditions are related not only to individual characteristics but also to job design, resource allocation, reporting systems, and the organization's response to ethical issues. Potipiroon & Wongpreedee [26] emphasize that an ethical climate must be accompanied by psychological safety so that employees feel empowered to report violations, while Magnusson et al. [25] demonstrate that an information security culture requires adequate organizational governance and resource support.

An ethical organizational culture in the digital transformation of public services at the Sumedang Regency Population and Civil Registration Office has developed quite well, but has not yet been fully internalized in a uniform and consistent manner. This culture is characterized by a commitment to integrity, accountability, fairness, empathy, data confidentiality, accuracy, and a service-oriented approach,

which are reflected in the behavior of leaders, division heads, staff, and operators, and are generally recognized by the public. Strengthening this culture requires consistent leadership by example, case-based ethics training, confidential reporting mechanisms that protect whistleblowers, realistic workload distribution, the provision of adequate equipment, and a balance between speed, accuracy, security, and humane service. Roy et al. [23] emphasize that a strong ethical culture is determined not only by statements of values but also by the alignment between organizational values, leadership behavior, work systems, and employees' experiences in dealing with ethical issues.

Accountability and Controlling

Accountability in *ethical governance* is the obligation of public officials and organizations to explain, take responsibility for, and accept the consequences of their decisions, actions, exercise of authority, and service outcomes to those who grant them their mandate and to the public as service recipients. Meanwhile, controlling is the process of monitoring, examining, evaluating, and correcting to ensure that the actions of public officials comply with regulations, service standards, codes of ethics, and the public interest. In public administration, accountability should not be interpreted merely as administrative reporting but must include clarity regarding responsible parties, traceability of decision-making processes, transparency of information, opportunities for the public to file objections, and corrective actions in the event of errors. Lestari [27] explains that digital transformation can strengthen accountability and transparency in the public sector through data recording, real-time reporting, and enhanced controlling capabilities; however, these benefits depend on the quality of governance, internal controls, and organizational capacity.

In the transformation of digital public services, accountability and controlling encompass individual, technical, organizational, and public dimensions. Individual accountability relates to the actions of officials or operators; technical accountability relates to security, reliability, and system activity logs; organizational accountability relates to the agency's obligation to provide standard operating procedures (SOPs), training, resources, and controlling; while public accountability relates to information transparency and the public's ability to monitor service delivery processes. Pullen et al. [19] emphasize that digital ethics governance requires structural, procedural, and relational mechanisms that can clarify responsibilities, decision-making processes, controlling, and accountability relationships between organizations and affected parties. Thus, technology must not obscure who is responsible when errors or losses occur in service delivery.

Accountability and controlling at the Sumedang Regency Population and Civil Registration Office have been implemented through the division of responsibilities, tiered controlling, the use of individual accounts, system activity logging, document reviews, correction mechanisms, and the handling of public complaints. Each stage of service has designated staff and officials responsible for it, while user actions can be reviewed via an *audit trail*. However, controlling still tends to be reactive, as in-depth reviews are more often

conducted after errors, disruptions, or complaints have occurred. Furthermore, internal accountability mechanisms have not yet been fully translated into information that the public can monitor. Magnusson et al. [25] explain that public sector information security governance must include risk management, an accountability framework, monitoring, compliance audits, security maturity assessments, and continuous organizational learning.

The Head of the Sumedang Regency Population and Civil Registration Office explained that controlling is carried out in a tiered manner, starting from operators, coordinators, administrators, division heads, up to the head of the office. Each user is granted access rights in accordance with their position and duties, while their activities can be reviewed through the system's audit trail. Data changes must be supported by valid documents and undergo verification and approval in accordance with the appropriate authority. Accountability is determined based on the source of the problem and the stage at which the error occurred. Input and verification errors are the responsibility of the staff members and reviewing officials; technical disruptions are handled by administrators and coordinated with the central system administrators; while cases of access misuse or data breaches are first investigated to determine user actions, system vulnerabilities, and the affected data. These practices demonstrate that accountability is not assigned to a single individual before the cause of the problem is identified, but rather encompasses individual, technical, and organizational responsibilities. Pullen et al. [19] emphasize that digital accountability requires a clear division of roles without eliminating the organization's responsibility for the systems and processes it uses.

The Head of the Division of Population Administration Information Management and Data Utilization at the Sumedang Regency Population and Civil Registration Office explained that user activity can be traced through account identifiers, access times, types of services, and actions taken on the data. These records are compared with supporting documents, application registers, and issued documents. If any unusual access or data changes outside the scope of a user's duties are detected, further clarification and investigation are conducted. Evaluations are also carried out through checks on active accounts, reviews of access rights, monitoring of disruptions, examination of complaints, and compliance checks against SOPs. However, the use of *audit trails* is still primarily conducted after an issue occurs and has not yet been fully analyzed on a regular basis to detect patterns of unusual access. Magnusson et al. [25] emphasize that effective information security governance does not rely solely on activity logging but also requires risk assessment, performance indicators, continuous monitoring, compliance audits, and security data analysis as preventive measures. Additionally, access rights must be adjusted in the event of personnel transfers, changes in duties, operator replacements, retirement, or employee termination. Although evaluations have been conducted, security testing and user compliance checks have not yet been fully scheduled or systematically documented. Coordination of controlling involves department heads, administrators, service divisions, the Directorate General of Population and Civil Registration, the

Sumedang Regency Communication, Information, and Information Technology Agency, the legal division, and other supervisory agencies as needed. This situation indicates the existence of a multi-stakeholder controlling structure, but its effectiveness still requires integrated scheduling, division of authority, documentation, and follow-up. Pakhnenko & Kuan [13] explain that accountability in digital government requires access controls, continuous controlling, clarity of authority, and the organization's ability to trace data usage at every stage of service delivery.

The Head of the Population Registration Services Division at the Sumedang Regency Population and Civil Registration Office stated that controlling of services related to the electronic ID card (KTP-el), Family Card (Kartu Keluarga), Child Identity Card (Kartu Identitas Anak), and population migration is carried out through on-site monitoring, document reviews, application logging, verification of the accuracy of results, processing times, public complaints, and system activity logs. Controlling indicators are not only focused on the number of completed documents but also cover data accuracy, the completeness of supporting documents, document security, staff conduct, and follow-up on problematic applications. A document correction mechanism is in place, but information regarding correction requirements, submission channels, correction status, and completion times still needs to be made more accessible. These conditions indicate that internal controlling has utilized both quantitative and qualitative indicators, but public accountability is not yet fully accessible. Mynenko & Lyulyov [28] explain that digitization can enhance the transparency of public institutions if technology is used to expand public access to information, processes, and the outcomes of government administration. Controlling of document issuance is conducted in a multi-tiered manner. The receiving officer is responsible for checking initial completeness; the verifier checks the identity and validity of the documents; the operator is responsible for the accuracy of data entry; and the authorized official ensures compliance with requirements before granting approval and providing an electronic signature. This division of roles provides clarity regarding responsibilities at each stage of service delivery. However, the organization remains accountable if errors occur due to unclear standard operating procedures (SOPs), insufficient training, unreasonable workloads, or system weaknesses. This demonstrates that accountability for digital services must not stop at identifying the staff member who made the error but must also assess the institutional factors that enabled the error to occur. Pullen et al. [19] emphasize that digital ethics governance must link individual accountability to organizational responsibility for system design, procedures, resources, and controlling mechanisms.

Population Administration Service Officers at the Sumedang Regency Population and Civil Registration Office confirmed that their work is monitored through file reviews, service outcomes, turnaround times, system activity, and public complaints. If an error stems from an officer's actions, it must be reported immediately, verified against source documents, corrected in accordance with procedures, and explained to the public. Officials also believe that the public should not be

burdened with additional procedures if errors stem from the service providers. Service evaluations are conducted through meetings, briefings, satisfaction surveys, and discussions of obstacles; however, these evaluations still focus more on the efficiency and quantity of services rather than ethical conduct and data security. This situation highlights the need to expand evaluation indicators from *output accountability* to *process and ethical accountability*. Lestari [27] explains that digital accountability in the public sector must integrate performance metrics, internal controls, information quality, compliance, and transparency so that accountability is not limited to quantitative outcomes.

The Digital Service System Operator at the Sumedang Regency Population and Civil Registration Office explained that every action within the system can be traced through the account, time of occurrence, device, transaction type, supporting documents, and service stages. When a disruption or suspected incident occurs, the operator must document the incident, secure the device and digital evidence, halt risky activities, and report it to the administrator or coordinator. Follow-up actions may include data correction, account deactivation, access restriction, counseling, disciplinary review, or referral to the appropriate authorities. However, scheduled, comprehensive, and documented security audits still need to be strengthened, as evaluations tend to be conducted only after disruptions, findings, or system changes have occurred. These practices indicate that traceability capabilities are available but have not yet been fully developed into preventive controlling. Magnusson et al. [25] emphasize that digital government systems require continuous risk assessment, monitoring, compliance audits, reporting, and security maturity evaluations to shift controlling from reactive to proactive.

Users of the Sumedang Regency Population and Civil Registration Office's digital services reported that communication and complaint channels are available and that complaints submitted directly generally receive a response. However, users do not always receive a receipt or a case number, making it difficult to track the progress of complaint resolution. Information on the status of applications also remains general, such as "being processed," without specifying whether the application is being verified, awaiting approval, requires corrections, or has already been issued. Explanations regarding rejections, delays, and errors are sometimes not provided in specific detail. These conditions indicate a gap between internal accountability mechanisms and the accountability that the public can observe. [21] explains that public trust in the government is influenced by their assessment of the effectiveness of e-services. Therefore, information regarding service status, reasons for decisions, and the progress of complaints needs to be communicated clearly and in an easily understandable manner.

Users of digital services also express confidence that data submitted through digital services is managed securely because it uses government systems. However, this confidence is not yet fully established because the public lacks detailed knowledge about how data is stored, who can access it, controlling of data usage, and the measures organizations take in the event of a data breach or misuse. This indicates that public trust is still largely based on the government's institutional status rather than on

knowledge of data protection mechanisms. Nurlinah et al. [17] found that positive perceptions of digital transformation can increase public trust, but its impact depends on service quality, transparency, security, and the public's experience when interacting with the government. Thus, transparency in data protection is necessary to transform trust that is based on assumptions into trust grounded in information.

Consistency regarding the division of responsibilities, tiered audits, the use of individual accounts, system activity logging, document verification, correction mechanisms, and error handling. This consistency indicates that accountability has been institutionalized within the service structure. Pullen et al. [19] explain that digital ethics governance becomes stronger when responsibilities, review procedures, controlling mechanisms, and correction channels are clearly defined and consistently implemented. The implementation of accountability and controlling has not yet been fully optimized. Audit trails have not been utilized proactively, security audits have not been scheduled consistently, access rights evaluations have not been fully documented, complaint tracking has not been integrated, and the status of follow-up actions is not transparent to the public. These conditions indicate that internal accountability has not yet fully transformed into public accountability. Mynenko & Lyulyov [28] emphasize that digitization will only enhance transparency if the information generated is accessible and can be used by the public to understand and monitor government actions. Therefore, the availability of data and activity logs must be accompanied by relevant mechanisms for reporting, analysis, and information disclosure.

Accountability and controlling in the digital transformation of public services at the Sumedang Regency Population and Civil Registration Office already have reasonably adequate mechanisms in place, but still require strengthening. This is evident in the division of responsibilities, individual accounts, *audit trails*, multi-tiered checks, hierarchical controlling, corrective mechanisms, complaint handling, and the imposition of sanctions commensurate with the severity of the violation. Strengthening these mechanisms requires periodic security audits, access pattern analysis, evaluation of access rights based on the civil service cycle, integration of complaint logging, assignment of report numbers, step-by-step status tracking, setting resolution deadlines, and transparency regarding the protection and handling of data misuse. Magnusson et al. [25] emphasize that information security governance in the public sector requires the integration of risk management, controlling, auditing, reporting, performance measurement, compliance, and organizational learning. With these enhancements, accountability is not only maintained within the organization but can also be observed, understood, and felt by the public.

Ethics Education and Communication

Ethics education in *ethical governance* is a systematic process designed to enhance civil servants' knowledge, moral sensitivity, decision-making abilities, and skills in resolving ethical dilemmas that arise while performing their governmental duties. Ethics education is not sufficient if it is limited to the

dissemination of codes of ethics, regulations, and prohibitions; rather, it must help public officials identify ethical issues, consider the impact of decisions on society, determine appropriate actions, and take responsibility for their actions. Caldwell et al. [29] found that ethics education using experiential learning is more effective in improving moral reasoning than methods such as lectures, material presentation, behavioral modeling, and role-playing that do not involve direct participant engagement. Therefore, ethics education for public officials needs to use cases that correspond to the service-related issues they actually face.

Ethical communication is the process of conveying and exchanging information regarding values, behavioral standards, authority, prohibitions, risks, and ethical responsibilities to public officials and the public. In digital public services, ethical communication encompasses internal communication regarding regulatory changes, standard operating procedures (SOPs), data usage, and incident management, as well as external communication regarding service procedures, data protection, fraud risks, and public rights. Communication is considered effective when information is not only conveyed but also understood and can be applied by the recipients. Sutalhis & Novaria [30] explain that digital literacy among public officials and the public encompasses digital skills, digital ethics, digital security, and digital culture. These four elements are necessary to prevent the misuse of information while improving the quality of public services.

Ethics education and communication at the Sumedang Regency Population and Civil Registration Office have been carried out through employee training sessions, leadership briefings, regulatory outreach, technical guidance, evaluation meetings, the signing of integrity pacts, and the dissemination of information to the public through various channels. The training materials have covered integrity, service ethics, data protection, non-discriminatory service, prohibition of illegal fees, use of personal accounts, and limitations on authority. However, digital ethics education is still largely combined with general guidance and technical training, so it has not yet been implemented in a specialized, structured, case-based, and periodic manner. Damanabi [31] indicate that case-based ethics learning can enhance ethical sensitivity because participants not only learn the norms but also learn to recognize and assess ethical issues in situations that resemble professional practice.

The Head of the Sumedang Regency Population and Civil Registration Office explained that ethics training is integrated with technical training on service delivery and system operation. Before carrying out their duties, employees and operators are provided with an understanding of their authority, responsibilities, prohibitions, risks associated with data use, public service ethics, the civil service code of conduct, integrity, prevention of discrimination, prohibitions on illegal fees, protection of personal data, confidentiality of population data, use of individual accounts, and access restrictions. This indicates that the organization views civil service competence as a combination of technical skills and ethical responsibilities. However, incorporating ethics material into technical training risks reducing ethical discussions to a mere add-on if not accompanied by dedicated time, specific methods, and

evaluation. Caldwell et al. [29] emphasize that the effectiveness of ethics training is influenced by instructional design and the level of participant engagement, not merely by the presence of ethics material in the training program.

The Head of the Division of Population Administration Information Management and Data Utilization at the Sumedang Regency Population and Civil Registration Office stated that the training provided to operators covered the operation of the Population Administration Information System, data verification and validation, account usage, access restrictions, document protection, and reporting of system disruptions. Changes to regulations, SOPs, and security risks were communicated via official letters, internal meetings, official communication groups, briefings, and explanations from administrators. However, training still tends to focus on technical skills, while material on *phishing*, *malware*, social engineering, account takeover, data breaches, and ethical dilemmas has not yet been provided comprehensively and systematically. Bishop et al. [32] explains that employees' cybersecurity awareness is determined not only by their knowledge of policies but also by their perception of threats, attitudes toward security, confidence in taking action, experience, and engagement. Therefore, digital security training needs to link knowledge with the skills to respond to threats in real-world situations.

A Digital Service System Operator at the Sumedang Regency Population and Civil Registration Office explained that handling disruptions and security risks is more often learned through daily experience and guidance from administrators after problems occur. Incident response simulations have not been conducted on a routine basis, even though operators need to practice dealing with compromised accounts, lost devices, misdirected documents, unusual access, *malware*, and suspected data breaches. Simulations are necessary so that operators know the initial steps to take, whom to contact, what digital evidence to secure, and what actions to avoid. Ho et al. [33] demonstrate that general annual security awareness training is not necessarily effective at changing employee behavior when facing *phishing*. These findings suggest that training must be supplemented with contextual exercises, repeated simulations, feedback, and behavioral evaluations so that security knowledge can be effectively applied.

The Head of the Population Registration Services Division at the Sumedang Regency Population and Civil Registration Office explained that staff members have received training on service standards, codes of ethics, service communication, discrimination prevention, data protection, and services for vulnerable groups. Staff members are instructed to provide assistance to the elderly, people with disabilities, and members of the public who are not tech-savvy. However, this training still needs to be expanded to include case studies, such as dealing with angry members of the public, suspected unauthorized use of identity, data requests by unauthorized parties, and the conflict between service speed and the thoroughness of verification. Damanabi [31] demonstrate that the use of professional case studies can enhance ethical sensitivity because participants are trained to recognize the moral dimensions of issues that cannot always be resolved

simply by following routine procedures. Thus, training for officers needs to develop their communication skills, situational judgment, empathy, and ethical decision-making.

The Head of the Civil Registration Services Division at the Sumedang Regency Population and Civil Registration Office added that officials need the ability to handle cases involving sensitive personal and family information. Officials need to be trained to communicate without judgment, maintain privacy, limit questions to relevant information, and explain missing requirements in an ethical manner. Officials must also understand the differences between delays, returning documents for correction, and rejections based on regulations, particularly in services related to divorce, child acknowledgment, child legitimation, adoption, identity changes, and family conflicts. These conditions demonstrate that service competencies are not merely administrative in nature but also require moral sensitivity and interpersonal communication skills. Caldwell et al. (2020) explain that experience-based learning helps participants develop moral reasoning when facing complex situations that cannot be resolved through rote memorization of formal regulations.

Population Administration Service Officers at the Sumedang Regency Population and Civil Registration Office confirmed that the training materials have helped them understand that digital service violations are not limited to data entry errors. Accessing data without a legitimate work-related purpose, allowing others to use one's account, storing documents on personal devices, and sending documents to the wrong recipient are also ethical and security issues. However, specialized training on digital ethics and personal data protection has not been conducted frequently, while forums specifically addressing ethical dilemmas have not been consistently available because such discussions are still combined with technical and operational evaluations. This situation indicates that the organization has established a foundation of knowledge but has not yet provided a space for reflective learning that allows employees to discuss ethical issues in depth. Damanabi [31] emphasize that ethical sensitivity can be enhanced through learning that provides participants with opportunities to analyze, discuss, and make decisions regarding professional cases.

Internal communication regarding changes to SOPs and policies has been conducted through meetings, direct briefings, official letters, documents, and work-related communication groups. However, the distribution of documents does not guarantee a shared understanding, as each staff member may interpret policies differently. Direct explanations, examples of implementation, question-and-answer sessions, demonstrations, and confirmation of understanding are necessary to ensure that policy changes are implemented consistently. Every change must also be promptly followed by updates across all service channels so that staff and the public do not receive conflicting information. Caldwell et al. (2020) indicate that passive learning methods have limitations in developing practical application skills, whereas direct engagement and experiential learning have a stronger influence on moral judgment. Therefore, internal communication must be two-way and provide opportunities for staff to test their understanding.

The Sumedang Regency Population and Civil Registration Office's Digital Service User Community explained that service information has been communicated through staff members, information displays at the office, official social media accounts, local government channels, and outreach activities. This information includes requirements, procedures, processing times, fees, service outcomes, and complaint channels. The public has also been reminded to use official channels and not to provide their National Identification Number (NIK), Family Card (Kartu Keluarga), e-ID card (KTP-el) photo, passwords, or verification codes to unknown parties. However, instructions such as "document does not match" and "file is incomplete" are not helpful enough if they are not accompanied by an explanation of what is wrong and how to correct it. The public still needs step-by-step guides, document examples, file formats, status tracking, estimated completion times, a list of official channels, information on fraud schemes, and procedures to follow if data has been provided to unauthorized parties. Amirulkamar [34] explains that digital literacy in public services encompasses the ability to use technology, understand digital ethics, maintain security, and foster a culture of responsible digital behavior. Therefore, public communication must provide practical knowledge that enables the public to use services safely.

Outreach and support have not yet reached all community groups equally, particularly those living far from service centers, those who do not actively use social media, the elderly, people with disabilities, and those with limited digital literacy. This situation indicates that service communication cannot rely solely on social media or digital applications but must involve subdistricts, villages, urban villages, neighborhood units (RTs), and community units (RWs). The simultaneous use of the official WhatsApp channel, websites, social media, telephone, print media, and local-level staff is better suited to the diverse capabilities of the public. Haerana & Riskasari [35] show that outreach, education, mentoring, and evaluation activities can improve the public's knowledge and skills in using digital public services. Thus, multichannel communication must be combined with direct mentoring to ensure that digital transformation does not widen the access gap.

Evaluations of ethics education and communication have been conducted through observation of staff behavior, compliance with SOPs, the number of errors, public complaints, satisfaction surveys, and evaluation meetings. However, these evaluations remain general in nature and have not yet utilized specific instruments to measure changes in civil servants' knowledge, attitudes, ethical sensitivity, and behavior. Evaluations are also more frequently conducted after errors or complaints have arisen. Pre- and post-training tests, case simulations, demonstrations, compliance audits, behavioral observations, and assessments of staff competence are necessary to objectively measure the effectiveness of training. Bishop et al. [32] explains that cybersecurity awareness is a construct that encompasses knowledge, attitudes, threat perceptions, self-confidence, experience, and behavior. Therefore, evaluation must go beyond simply measuring participant attendance or cognitive mastery of the material.

Ethics education and communication have become an integral part of civil service training and the delivery of digital services. Caldwell et al. [29] emphasize that ethics education is more effective when designed as an active learning process that connects values, experiences, and decisions within the context of participants' work.

Ethics education and communication in digital services at the Sumedang Regency Population and Civil Registration Office are not yet fully optimized. Ethics education is still largely integrated into technical training; it is not yet conducted on a regular basis or based on case studies, is not supported by incident simulations, and is not evaluated using measurable instruments. Communication with the public also does not fully explain data security, digital risks, the reasons for document returns, processing stages, and actions to take in the event of misuse. Ho et al. [33] indicate that routine and general security training does not always result in behavioral change, while Sutalhis & Novaria [30] emphasize the importance of integrating skills, ethics, security, and digital culture. These findings suggest that ethics education and communication need to shift from merely conveying information toward building competencies and fostering appropriate behavior.

Strengthening ethics education and communication at the Sumedang Regency Population and Civil Registration Office should focus on periodic training programs, specialized modules on digital ethics, case-based learning, security incident simulations, forums for discussing ethical dilemmas, and evaluations of civil servants' knowledge, attitudes, and behavior. On the community side, guidelines are needed that are simple, consistent, easily verifiable, and available through various media, accompanied by expanded guidance through subdistricts, villages, urban villages, neighborhood units (RTs), and community units (RWs). Damanabi [31] demonstrate that case-based learning can enhance ethical sensitivity, while Haerana & Riskasari [35] emphasize the importance of outreach, education, and evaluation in improving the public's digital literacy. With these reinforcements, ethics education and communication will not only serve as a means of conveying rules but also as an instrument for shaping the behavior of public officials and empowering the public to use digital services safely and responsibly.

4. CONCLUSION

Ethical leadership in the implementation of *ethical governance* during the digital transformation of public services at the Sumedang Regency Population and Civil Registration Office has been reflected in the exemplary conduct of leaders, adherence to procedures, data protection, document accuracy, fairness in service delivery, and consideration for members of the public facing digital barriers. Leaders have prioritized the security and validity of documents as a crucial aspect of digital services, rather than merely pursuing speed in processing. However, implementation has not yet been fully optimized, as consistency in following up on complaints, the speed of assistance, the simplicity of procedures, and the equitable distribution of alternative services still need to be strengthened

so that the organization's ethical commitment can be felt equally by the public.

Standards and codes of ethics already have a sufficiently strong regulatory and operational foundation through laws and regulations, service standards, SOPs, service announcements, civil service codes of ethics, integrity pacts, access restrictions, the use of individual accounts, and multi-layered verification. These various instruments have served as guidelines for civil servants in providing services and managing population data responsibly. Nevertheless, the existing standards do not yet fully address the evolving issues of digital ethics and security risks. Updates to SOPs, guidelines for handling ethical dilemmas, incident response procedures, and the dissemination of information regarding data use and protection to the public are still needed to strengthen ethical digital public services.

An ethical organizational culture has developed through a commitment to integrity, honesty, professionalism, responsibility, fairness, empathy, prudence, data confidentiality, and a service-oriented approach. These values are reflected in the behavior of leaders, division heads, staff members, and operators, and are reinforced through practices such as cross-checking, mutual reminders, assisting the public, safeguarding documents, and correcting service errors. However, this ethical culture has not yet been fully internalized in a uniform and consistent manner, particularly when staff face heavy workloads, resource constraints, system disruptions, and pressure to meet service targets. Leadership by example, protection for whistleblowers, realistic division of labor, and the provision of adequate work resources still need to be strengthened so that ethical behavior becomes a sustainable organizational norm.

Accountability and controlling have been implemented through the division of responsibilities, the use of individual accounts, system activity logging, multi-tiered document reviews, tiered controlling, correction mechanisms, complaint handling, and the imposition of sanctions commensurate with the severity of the violation. Accountability is not only assigned to individual staff members but also encompasses technical and organizational responsibilities for providing systems, SOPs, training, and adequate controlling. However, the use of *audit trails* still tends to be reactive, security audits are not consistently scheduled, complaint tracking is not yet integrated, and the status of follow-up actions is not fully transparent to the public. Controlling needs to be developed to be more proactive, documented, measurable, and easily monitored by service users.

Ethics education and communication have been implemented through employee training sessions, leadership briefings, regulatory outreach, technical guidance, evaluation meetings, integrity pacts, and the dissemination of service information through various media. Training materials have covered integrity, non-discriminatory service, limits of authority, data protection, account usage, and digital document security. However, ethics education is still largely combined with technical training; it has not been conducted specifically or on a regular basis; it has not utilized case-based learning or incident simulations; and it has not been evaluated using measurable instruments. Communication with the public also needs to be made simpler, more detailed, and consistent, and it

must reach groups with limited digital access so that the transformation of digital public services proceeds safely, inclusively, transparently, and ethically.

REFERENCES

- [1] I. Y. Kurniawan, T. Prasetyowati, and B. A. Kurniawan, "Etika Pelayanan Publik Untuk Mewujudkan Good Governance di Polres Pelabuhan Tanjung Perak Kota Surabaya," *Jurnal Administrasi Publik dan Ilmu Komunikasi*, vol. 12, no. 2, pp. 249-258, 2025. doi: 10.55499/intelektual.v12i2.1643.
- [2] Nastia, "TRANSFORMASI DIGITAL MELALUI INOVASI E-GOVERNMENT PADA PEMERINTAH DAERAH KABUPATEN BUTON SELATAN," *Governance*, vol. 12, no. 2, pp. 268-281, 2024. doi: 10.33558/governance.v12i2.9799.
- [3] S. Sasfiani, R. Putra, K. Imania, and A. Iriani, "Tantangan dan Strategi Implementasi Chatbot Government Transformasi Administrasi Digital di Indonesia," *Jurnal Pemikiran dan Penelitian Bidang Administrasi Sosial, Humaniora dan Kebijakan Publik*, vol. 8, no. 4, pp. 780-792, 2025.
- [4] R. Juwandi, D. Sundawa, P. Bestari, and S. Syaifullah, "Transformasi Digital Pelayanan Publik: Urgensi Penguatan Etika dan Karakter dalam Kebijakan Inovatif di Banten," *Jurnal Moral Kemasyarakatan*, vol. 10, no. 2, 2025. doi: 10.21067/jmk.v10i1.11019.
- [5] R. Nggilu, and R. Mokodongan, "Model Manajemen SDM Publik Berbasis Kompetensi Digital dan Etika Pelayanan Publik (Studi Konseptual pada Dinas Kepegawaian Kota Gorontalo)," *Jurnal Agregasi : Aksi Reformasi Government dalam Demokrasi*, vol. 14, no. 1, pp. 111-127, 2026. doi: 10.34010/agregasi.v14i1.19144.
- [6] D. Halim, H. Herman, A. C. Susilawati, P. R. Adawiyah, N. I. Has, and Zumarina, "Etika Pelayanan Publik di era Digital Governance: Kajian Filsafat Administrasi Publik," *The Indonesian Journal of Public Administration*, vol. 11, no. 2, pp. 41-55, 2025.
- [7] C. Dinata, "Ethical Transformation in Public Administration in the Digital Era," *Journal of Social, Policy and Development Studies*, vol. 1, no. 2, pp. 9-17, 2024. doi: 10.65119/jspds.v1i2.15.
- [8] S. Rahmawati, and D. Nowanda, "Peran Etika dalam Mewujudkan Good Governance," *Jurnal Riset Multidisiplin Edukasi*, vol. 2, no. 1, pp. 324-333, 2025.
- [9] D. C. Menzel, *Ethics Management For Public Administrators: Building Organizations Of Integrity*. M.E. Sharpe, 2007.
- [10] R. K. Yin, *Case Study Research and Applications: Design And Methods* (6th Ed.). SAGE Publications, 2018.
- [11] Sugiyono, *Metode Penelitian Kualitatif*. Alfabeta, 2020.
- [12] X. Bian, and B. Wang, "Enabling Innovative Governance: Ethical Leadership and Dynamic Capabilities in Government Digital Transformation," *Business Ethics and Leadership*, vol. 8, no. 4, pp. 186-200, 2024. doi: 10.61093/bel.8(4).186-200.2024.
- [13] O. Pakhnenko, and Z. Kuan, "Ethics of Digital Innovation in Public Administration," *Business Ethics and Leadership*, vol. 7, no. 1, pp. 113-121, 2023. doi: 10.21272/bel.7(1).113-121.2023.

- [14] J. K. Jha, and M. Singh, "Exploring the mechanisms of influence of ethical leadership on employment relations," *IIMB Management Review*, vol. 31, no. 4, pp. 385-395, 2019. doi: 10.1016/j.iimb.2019.07.010.
- [15] H. Halbusi, K. A. Williams, T. Ramayah, L. Aldieri, and C. P. Vinci, "Linking ethical leadership and ethical climate to employees' ethical behavior: the moderating role of person-organization fit," *Personnel Review*, vol. 50, no. 1, pp. 159-185, 2021. doi: 10.1108/PR-09-2019-0522.
- [16] M. Ciesielska, N. Rizun, and J. Chabik, "Assessment of E-government inclusion policies toward seniors: A framework and case study," *Telecommunications Policy*, vol. 46, no. 7, Art. no. 102316, 2022. doi: 10.1016/j.telpol.2022.102316.
- [17] Nurlinah, M. C. Ansar, and K. Chowdhury, "Impact of government digital transformation on citizen trust and participation: evidence from Gowa Regency, Indonesia," *Frontiers in Human Dynamics*, vol. 7, 2025. doi: 10.3389/fhumd.2025.1700582.
- [18] R. Ahmad, R. A. Hashim, and A. R. Abdul Latiff, "ETHICAL BEHAVIOUR AND INTEGRITY AMONG EMPLOYEES IN THE PUBLIC SECTOR: A CRITICAL REVIEW," *International Journal of Entrepreneurship and Management Practices*, vol. 7, no. 25, pp. 467-496, 2024. doi: 10.35631/IJEMP.725036.
- [19] E. Pullen, E. Ruijter, and A. Meijer, "Governing Ethics for the Digital Transformation: Developing, Testing, and Validating a Framework," *Government Information Quarterly*, vol. 43, no. 2, Art. no. 102117, 2026. doi: 10.1016/j.giq.2026.102117.
- [20] Z. Khamzina, Y. Buribayev, and Y. Tileubergenov, "Institutionalizing integrity: rethinking ethical and cultural standards in Kazakhstan's civil service," *Frontiers in Political Science*, vol. 7, 2025. doi: 10.3389/fpos.2025.1573608.
- [21] S. Lee-Geiller, "The moderating effect of digital literacy on the link between e-government effectiveness and trust in government," *Journal of Policy Studies*, vol. 39, no. 4, pp. 77-101, 2024. doi: 10.52372/jps.e672.
- [22] V. Figueroa, L. E. Sánchez Crespo, A. Santos-Olmo, D. G. Rosado, and E. Fernández-Medina, "Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals," *International Journal of Information Security*, vol. 24, no. 3, Art. no. 121, 2025. doi: 10.1007/s10207-025-01024-0.
- [23] A. Roy, A. Newman, H. Round, and S. Bhattacharya, "Ethical Culture in Organizations: A Review and Agenda for Future Research," *Business Ethics Quarterly*, vol. 34, no. 1, pp. 97-138, 2024. doi: 10.1017/beq.2022.44.
- [24] Z. Wal, and M. A. Demircioglu, "More ethical, more innovative? The effects of ethical culture and ethical leadership on realized innovation," *Australian Journal of Public Administration*, vol. 79, no. 3, pp. 386-404, 2020. doi: 10.1111/1467-8500.12423.
- [25] L. Magnusson, S. Iqbal, P. Elm, and F. Dalipi, "Information security governance in the public sector: investigations, approaches, measures, and trends," *International Journal of Information Security*, vol. 24, no. 4, Art. no. 177, 2025. doi: 10.1007/s10207-025-01097-x.
- [26] W. Potipiroon, and A. Wongpreedee, "Ethical Climate and Whistleblowing Intentions: Testing the Mediating Roles of Public Service Motivation and Psychological Safety Among Local Government Employees," *Public Personnel Management*, vol. 50, no. 3, pp. 327-355, 2021. doi: 10.1177/0091026020944547.
- [27] P. A. Lestari, "Transparency and Accountability in the Digital Era: Insights from Public Sector Accounting," *Sinergi International Journal of Accounting and Taxation*, vol. 3, no. 3, pp. 195-208, 2025. doi: 10.61194/ijat.v3i3.864.
- [28] S. Mynenko, and O. Lyulyov, "The Impact of Digitalization on the Transparency of Public Authorities," *Business Ethics and Leadership*, vol. 6, no. 2, pp. 103-115, 2022. doi: 10.21272/bel.6(2).103-115.2022.
- [29] J. L. Caldwell, A. Y. Ortiz, E. R. Fluegge, and M. J. Brummett, "The Effectiveness of Ethics Training Strategies: Experiential Learning for the Win," *International Journal of Business and Management Research*, vol. 8, no. 4, pp. 124-131, 2020. doi: 10.37391/IJBMR.080407.
- [30] M. Sitalhis, and E. Novaria, "Literasi Digital dna Pelayanan Publik yang Baik," *Jurnal Inovasi Riset Akademik*, vol. 4, no. 1, pp. 17-24, 2024.
- [31] S. Damanabi, "The Impact of Professional Ethics Case-Based Learning on The Ethical Sensitivity of Health Information Technology Students," *Perspectives in Health Information Management*, vol. 21, no. 1, 2024.
- [32] L. M. Bishop, P. M. Asquith, and P. L. Morgan, "The Employee Cybersecurity Awareness Framework," *Human Behavior and Emerging Technologies*, vol. 2025, no. 1, 2025. doi: 10.1155/hbe2/1025045.
- [33] G. Ho, A. Mirian, E. Luo, K. Tong, E. Lee, L. Liu, et al., "Understanding the Efficacy of Phishing Training in Practice," *2025 IEEE Symposium on Security and Privacy (SP)*, pp. 37-54, IEEE, 2025. doi: 10.1109/SP61157.2025.00076.
- [34] S. Amirulkamar, "Penarapan Artificial Intelligence (AI) dalam Sistem Administrasi Publik: Peluang, Tantangan, dan Etika Pelayanan Publik di Indonesia," *The Journalish: Social and Government*, vol. 5, no. 1, pp. 87-94, 2024.
- [35] H. Haerana, and R. Riskasari, "Literasi Digital dalam Pelayanan Publik," *Jurnal Pengabdian Masyarakat Wikrama Parahita*, vol. 6, no. 2, 2022.