Preprints.org

Article

Not peer-reviewed version

Intentional Insider Threats to Data Security: A Mitigation Strategy for Municipalities

Shandukani Thenga * and S. Arunmozhi Selvi

Posted Date: 14 November 2025

doi: 10.20944/preprints202511.1091.v1

Keywords: Inside threats; data security; cybersecurity frameworks; risk management, personally identifiable information; NIST SP 800-53; Socio-technical mitigation; Organizational culture; Employee monitoring

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

Intentional Insider Threats to Data Security: A Mitigation Strategy for Municipalities

Shandukani Tshilidzi Thenga * and S Arunmozhi Selvi

British University College, Dubai, United Arab Emirates

* Correspondence: shandukanit90snr@gmail.com

Abstract

Municipal governments are the custodians of large volumes of sensitive information, including personally identifiable information (PII), financial information, law enforcement intelligence, and control of essential infrastructure. Although external cyber threats are the most discussed threats to data security, deliberate insider threats—malicious actions of authorised personnel in other words—are an equally serious but underestimated threat to municipal data security. This paper presents the holistic formulation of a mitigation strategy specific to local government settings. The proposed solution, based on standard frameworks such as NIST SP 800-53, ISO/IEC 27001, and the CERT Insider Threat Model and incorporating socio-technical and risk management concepts, consists of a multi-layered defence. Focusing on active prevention, ongoing surveillance, and organised incident recovery and response, this model is a combination of governance policies, technical controls, behavioural monitoring, and organisational culture reforms. In addition to presenting the model, this paper will cover a number of important ethical and legal issues, particularly the question of how to strike a balance between the privacy of employees and the monitoring required. A gradual implementation scheme and performance indicators are then proposed to guarantee feasible implementation, which is based on municipal budget and regulatory factors. Our study builds on earlier findings that insider risk mitigation extends beyond technology, forming a complex and culture-entrenched challenge that requires an overhaul of present municipal operations in order to instil trust, provide accountability, and enhance resilience.

Keywords: inside threats; data security; cybersecurity frameworks; risk management; personally identifiable information; NIST SP 800-53; Socio-technical mitigation; organizational culture; employee monitoring

1. Introduction

Municipal governments handle large quantities of sensitive government information that ensures that city operations run smoothly. This information consists of personal citizen data, tax and financial data, police databases, and data from the systems that manage utilities and transportation, and it must be kept safe in order to ensure the trust of the population and fulfil legal requirements. Although most organisations are concerned with cyberattacks by external hackers, insider threats posed by individuals within an organisation can be as harmful as external attacks. These attacks occur when workers or contractors gain access to information through their privileged access and abuse it to steal information, cause disruptions, or leak information. Local governments are particularly vulnerable, given that they usually have small budgets, outdated computer systems, and numerous departments, sharing data across various networks. Security problems can also be a challenge when political pressures or excessive competing priorities are present [1]. Even a single insider attack can be highly damaging, with consequences such as data loss, service interruption, and destruction of population trust.

The aims of this paper were to create a holistic insider threat prevention and response plan that is designed for municipal governments and to illustrate that proper protection demands not only

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

proper technology but also proper leadership, clear policies, awareness of employees, and a culture of responsibility and security.

The rest of the paper is organised in the following way. Section 2 presents a literature review and theoretical framework of insider threats in municipal settings. Section details the type and effects of deliberate insider threats within municipalities. Section 4 explores the suggested methodology, which will include the risk assessment framework and multi-layered mitigation strategy. Section 5 deals with implementation considerations, ethical and legal issues, and resource planning. Lastly, Section 6 presents conclusions and recommendations for the leaders of the municipality.

2. Literature Review and Theoretical Framework

Insider threats are among the largest and most enduring issues of cybersecurity, particularly when they concern city governments that have access to public information, financial systems, and local infrastructures. These threats are perpetrated by individuals who already have access to systems, making them difficult to detect. Additionally, some insiders have ill-intentioned motives, whereas others cause harm unintentionally [2]. Researchers assert that insider threats must be addressed both technologically and humanly, through a combination of technological solutions, behavioural insights, and effective leadership [3,4].

2.1. Defining Insider Threats and Context

According to the literature cited above, insider threats can be divided into two categories: malicious and non-malicious. Malicious insider threats involve incidents when someone intentionally steals information, destroys systems, or defrauds, whereas non-malicious insider threats are inadvertently harmful, usually as a result of neglect. Alsowail and Al-Shehari [3] proposed a model that integrates technology, behavioural insights, and organisational practices to curb insider threats. They explained that tools such as access control or system monitoring cannot exist independently. Powerful recruitment, reference checking, and moral consciousness are also required. This is particularly true in municipalities that rely on outdated systems and minimal IT personnel.

These challenges are exacerbated in the case of municipal governments, which often have limited budgets and operate via numerous departments. Vestad and Yang [5] discovered that the majority of local governments use cybersecurity plans developed by national or personal agencies without modifying them to suit local requirements. The consequences of this are usually poor supervision, inadequate access control, and inadequate monitoring of insider operations.

2.2. Organisational and Behavioural Dimensions

Human factors are the key contributors to insider threats. Safa and Abroshan [6] discovered that transparency in leadership, employee motivation, and a feeling of equity have a significant influence on whether employees are likely to behave responsibly, indicating that when employees feel trusted and valued, they are unlikely to damage an organisation. This applies especially in city offices where strict management styles may hinder organizational communication and accountability.

Steinmetz et al. [4] further notes that organisations can promote insider advocates—this refers to employees who promote security, report risks, and develop good behaviour. This concept relates to Social Exchange Theory, according to which organisations should treat employees fairly, and, in return, employees then offer their loyalty and sincerity. Municipal leaders can apply this concept by promoting fairness, inclusion, and open communication in order to minimise the possibility of insider threats.

2.3. Technical and Procedural Frameworks

Technology remains essential in combating insider threats and has to enable prompt detection and response. According to Savchenko et al. [7], damage is enhanced in the event of slow

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

technological responses; thus, constant monitoring and automatic notifications should be implemented in order to ensure that IT teams can respond with greater speed and precision.

Moreover, Nagel [8] suggests that cities implement a formal, regularly updated programme for insider threats. The Information Systems Audit and Control Association (ISACA) model is geared towards governance, training, detection, and response; as far as local governments are concerned, this model would provide a means of incorporating insider threat management into a cybersecurity policy, with clear coordination protocols and periodic review.

2.4. Municipal Data Environment and Emerging Challenges

Research has found that municipal cybersecurity has become more complicated due to new smart city systems. According to Cornelius and Van Rensburg [9], because weak authentication, low accountability, and poor data governance contribute to risks, zero-trust and privacy-by-design practices are recommended, whereby no one is trusted. Vestad and Yang [5] additionally mention that outside contractors are dangerous, as they can gain extensive access without appropriate control measures. Cities can address this by revising vendor access on a regular basis and executing more robust contracts.

2.5. Synthesis and Implications

In general, research indicates that the security of municipal data requires both human and technical strategies. Alsowail and Al-Shehari [3] emphasise technical controls, Safa and Abroshan [6] emphasise the importance of the organisational culture, and Steinmetz [4] introduces the concept of positive engagement among employees. Moreover, Savchenko et al. [7] emphasise the necessity of faster responses, whereas Cornelius and Van Rensburg [9] highlight the risks posed by smart cities. When these studies are combined, they demonstrate that integrating insights from policy-, culture-, and technology-based perspectives can assist municipalities in minimising insider threats and ensuring trust from the population. Moreover, Saxena et al. [23] state that situational awareness, constant monitoring, and responsibility are key to preventing insider threats in organisations and critical businesses.

3. The Nature and Impact of Intentional Insider Threats in Municipalities

Municipal governments are especially vulnerable to malicious insider threats, as these threats are committed by people who have trusted, legitimate access to the system. Common insider personnel include IT administrators, finance officers, human resources, and hired vendors who access sensitive municipal information or maintain important systems [4]. Such individuals can access the system to harm, steal, or manipulate data. The National Whistleblower Centre [24] explains that the Fraud Triangle (opportunity, pressure, and rationalisation) framework helps identify the reason insiders commit harmful acts, while EverEdge Global [24] describe that the Money, Ideology, Coercion, and Ego (MICE) models is another approach to understand insider motivation [3,4]. In municipalities, multiple opportunities for malicious insider threats exist, with multiple entry points and minimal control provided by complex and decentralised systems [3].

Municipalities are more prone to structural, technical, and procedural weaknesses, with past infrastructure and departmental IT setups complicating the process of establishing consistent access control, monitoring, and patch management [5]. Moreover, many municipalities primarily rely on contractors or suppliers of specialised IT support, which raises the issue of the extended insider. These third parties can have the same (or even higher) system permissions than employees, yet they are often not subject to routine security checks [9]. Another complication is the lack of resources. Local governments often have limited cybersecurity funds and a small technical team and experience struggles to maintain continuous efforts to monitor personnel, train staff, and respond to incidents [6].

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

The scope of municipal insider threat impacts extends to operational, financial, and reputational spheres. Insiders can behave maliciously on a technological scale via data exfiltration, misuse of privileges, or sabotage of operational technology [7]. Monetary implications encompass direct remediation costs, litigation, and the cost of restoring citizen services. Nevertheless, loss of public trust is usually the greatest damage caused in the long run, as the loss of personally identifiable information (PII) or key service data of citizens harms their confidence in local governance. This last consequence is difficult to measure and lies at the core of municipal legitimacy [5].

The case of Terry Childs in 2008 in San Francisco is a well-known example of how insider threats can have a devastating effect on a city government [8]. Childs, a senior network administrator, declined to hand over the passwords of the FiberWAN network in the city that linked over sixty departments. This caused city officials to be locked out of their systems for a few days and brought about many service inconveniences, costing the city millions of dollars to remedy. Nagel [8] claims that this event demonstrated that San Francisco's privileged accounts were poorly managed, the job roles were not separated, and the work culture was conducive to providing excessive, unregulated authority to IT personnel. Furthermore, this incident demonstrated that a lack of proper checks in place, where one individual has too much control, can place an entire municipal network at risk.

In general, insider threats in city governments occur when valuable information, poor management, and personal desires converge. Although more focus is given to outside hackers, insiders may inflict even more damage due to their trusted access to systems [3,6]. Consequences of insider threats extend beyond lost data; the damage caused by malicious behaviour may undermine public confidence, destroy vital services, and cause long-term issues in a city. **Figure 1** depicts the standard insider threat lifecycle in municipal settings and how the insider threat may enter the network initially as a legitimate employee and then potentially be detected and stopped. This cycle shows how insider threats can be sustained unless it is dealt with effectively through a continuous monitoring and improvement process. Given this, it is important that municipalities develop well-developed and balanced protection strategies comprising technology, employee training, and organisational responsibility.

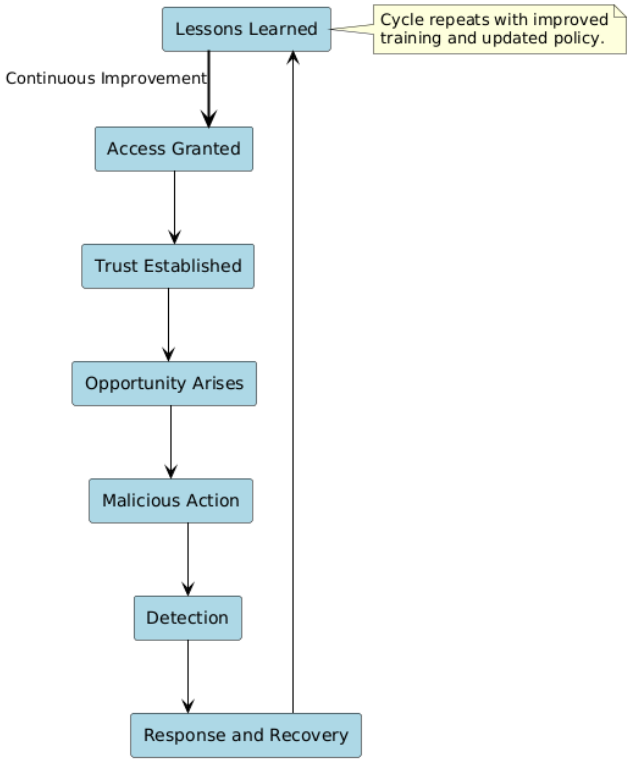

Figure 1. Insider threat lifecycle.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

4. Methodology

4.1. Risk Assessment Framework for Municipal Insider Threats

Municipalities must develop a viable risk assessment model that would help them detect, analyse, and address insider threats in a systematic manner. Given that municipal institutions work in an interrelated and data-rich environment, the systematic approach chosen must ensure that both technical and human risk factors are addressed. The following framework incorporates a combination of situational awareness, behavioural analysis, and adaptive risk modelling in order to offer a practical and evidence-based methodology for insider risk identification.

4.1.1. Asset Identification and Situational Awareness

The initial process of evaluating insider threats involves mapping municipal assets, users, and data flows in order to identify how information flows across departments and systems. Chandra et al. [10] emphasise that situational awareness frameworks should assist organisations in visualising user–system and data interaction relationships. At a municipal level, this would entail the definition of key datasets, such as citizen personal records, financial information, and infrastructure control data, and establishing who should have authorised access to these and by whom. Using the principles of situational awareness, municipalities can then identify access anomalies and exposure points before they become exploitable.

4.1.2. Human and Technical Risk Modelling

After the documentation of assets and data flows, municipalities should simulate insider threat cases by utilising a human-based risk approach. Zeng and Dian [11] suggest a model, known as the Insider Human Factors Analysis and Classification System-Bayesian Network (IHFACS-BN), that calculates the probability of insider risks by combining psychological, organisational, and environmental factors [12]. This model allows municipalities to evaluate the possibility of increasing the risk of insider incidents due to employee stress, weak supervision, or poor policy enforcement. Combined with a likelihood-versus-impact matrix, this strategy will enable decision-makers to make mitigation decisions concerning the most critical vulnerabilities.

4.1.3. Dynamic and Explainable Risk Management

In the fast-changing digital space, static risk evaluation is insufficient. Islam et al. [13] suggest the use of intelligent, dynamic cybersecurity systems based on AI-driven analytics for real-time tracking, set against the backdrop of explainability and interpretability. These systems can detect abnormal behaviour—such as mass file access or inconsistent privilege utilisation—and deliver interpretable information that helps a security team make informed decisions. This adaptive approach would enable municipalities with available human resources to be more effectively responsive without exposing staff to false positives.

4.1.4. Socio-Technical Integration and Governance

Lishchynsky [14] highlights the fact that insider threat prevention must involve a socio-technical approach, with human, organisational, and technological aspects. This socio-technical approach implies that municipalities should integrate human, managerial, and technical activities into a single coordinated system. As an illustration, cybersecurity units should collaborate closely with human resources, as well as legal and management teams, to gain better insight into behavioural red flags before they develop into critical issues. Frequent employee training, background checks, and other explicit offboarding practices can help minimise risks, as only trusted and verified people would have system access.

Simultaneously, user behaviour must be constantly monitored via technical protection measures, including access control, system monitoring, activity logs. A combination of social

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

awareness and technology can result in cities developing a balanced, flexible, and effective insider threat defence suited to the realities of work in the public sector.

Table 1 provides an overview of the most important risk factors of insider threats in municipalities according to the organisational, human, and technical aspects. Such risk factors should be understood in order to develop specific mitigation measures.

Table 1. Risk factors for insider threats in municipalities.

Category	Key Risk Factors	Specific Controls
Organisational	Lack of oversight, weak policies, and decentralisation	Lack of admin privilege review
Human	Disgruntled employees, personal stress, and low morale	Employee anger about demotion
Technical	Legacy systems, excessive privileges, and poor logging	Old servers with weak access controls

4.2. Multi-Layered Mitigation Strategy

A multi-layered approach involving effective leadership, safe technology, employee participation, and recovery plans is a vast area in municipal governments where insider threats can be reduced. The defence-in-depth principle can be reflected in each layer, with each providing defence mechanisms against careless or malicious insiders. This section presents a systematic framework that can be adopted by municipalities, based on the current state-of-the-art research and best practices.

4.2.1. Governance and Policy Controls

4.2.1.1. Establishing an Insider Threat Programme

An effective insider threat strategy begins with effective governance. City governments should develop an official programme that would specify the roles of IT, HR, legal departments, and public safety departments, as well as how they should be organised. In accordance with NIST [15], who states that an insider threat management programme must be incorporated within an overall cybersecurity framework with leadership support, bringing departments together would support comprehensive monitoring and allow for a more streamlined execution of tasks.

4.2.1.2. Role-Based Access and Least Privilege

Role-based access control (RBAC) and the principle of least privilege are quite critical in minimising insider threats. Municipal IT systems are likely to be distributed among numerous departments; therefore, access must be limited to what is required by each employee. NIST [15] recommends access enforcement and the separation of duty control to reduce risks related to privilege abuse. Frequent reviews of access rights, especially after employees transfer or leave, would ensure that no orphaned accounts or those with unauthorised access continue to exist in the system.

4.2.1.3. Personnel Security and Offboarding Procedures

According to Safa and Abroshan [6], insider attacks may escalate when employees are dissatisfied and experience stress. Thus, background checks, regular testing of sensitive positions, and secure offboarding that terminates access upon employment termination should be used as personnel security measures by municipalities. Additionally, making HR policies consistent with cybersecurity policies would ensure accountability during the duration of employment in an organisation.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

4.2.1.4. Data Classification and Data Handling Policies

Given that municipalities are responsible for handling highly sensitive information, such as records of citizens and financial records, a policy on data classification would assist in identifying information deemed to be the most secure. NIST [15] states that labelling sensitive data, establishing retention regulations, and securely erasing old files are keys to ensuring that data protection strategies remain proportionate to the risks involved. Additionally, response teams must also be guided by these policies when recovering from an incident.

4.2.2. Technical and System Controls

4.2.2.1. Prevention: Patch Management, Authentication, and Segmentation

Given that safe systems are a starting point for prevention, multi-factor authentication (MFA), frequent updates to software, and network segmentation would restrict insiders from accessing critical systems (utilities and payroll). These measures minimise the possibility of insider abuse and contribute to sealing security breaches [16].

4.2.2.2. Detection: Analytics and Behavioural Monitoring

Prevention is essential, but early detection of suspicious behaviour is also important. In order to detect abnormal activity, such as the transfer of large amounts of data or late-night access, tools such as Security Information and Event Management (SIEM) and User and Entity Behaviour Analytics (UEBA) can be used. According to Savchenko et al. [7], the time lag between malicious activity and its detection can be minimised by real-time monitoring, which then minimises the total harm caused as a result. Nevertheless, cities should ensure that these systems are in line with privacy and labour laws [17].

4.2.2.3. Deterrence: Privileges, Access Control, and Auditing Records

Technical deterrence measures include privileged access management (PAM) systems, which contain administrative privileges, provide logging of session use, and generate unalterable audit trails. These are useful, as the perception of constant monitoring is a deterrent since it raises the risk of being caught. Moreover, extensive auditability not only is useful in investigations but also offers evidence of due diligence, which is crucial in terms of social responsibility [15].

4.2.3. Human and Behavioural Controls

4.2.3.1. Role-Specific Security Awareness Training

As the most vulnerable part of any system is human error [18], periodic, role-based training should be implemented in order to ensure that staff are aware of warning signs and how insiders can become threats. Trained employees on security concerns are less prone to making mistakes, being negligent, or engaging in suspicious activity [6].

4.2.3.2. Promoting a Positive Security Culture

Surveillance is not the sole aspect of insider threat prevention. To avoid frustration and isolation, municipal leaders ought to enhance fairness, transparency, and open communication. Safa and Abroshan [6] discovered that organisational trust reduces the risk of insider incidents, with a culture of verified trust making employees responsible yet not over-policed.

4.2.3.3. Reporting Mechanisms and Whistleblower Protections

Municipalities should establish secure and confidential ways through which employees can report suspicious activities. Whistleblower policies can serve to protect individuals against retaliation after disclosing concerns. A trained team should review any disclosure reports fairly. Moreover,

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

integrating reporting systems and monitoring would enhance prompt detection efforts and cement employee trust in security procedures.

4.2.4. Incident Response and Recovery Controls

4.2.4.1. Planning Insider-Specific Responses

Conventional response strategies consider external attacks, but insider attacks demand discretion. Thus, municipalities must formulate silent and organised reactions that minimise interference but gather evidence. NIST [15] suggests open communication between IT, HR, and legal divisions to ensure that all departments involved in the response process are familiar with the responsibilities undertaken by each role in this effort.

4.2.4.2. Forensic Preparedness and Law Enforcement Preparedness

IT personnel should be able to gather digital evidence by collecting logs and protecting systems after a breach. Operating in collaboration with law enforcement agencies would provide a means of ensuring that investigations are conducted in a manner that is legal and free of any corruption. This preparedness would be time-saving and would assist the city in fulfilling any disclosure requirements.

4.2.4.3. Continuous Improvement and Post Incident Recovery

After restoring the affected systems, leaders should analyse what went wrong and reformulate policies or training accordingly. According to [7], incident recovery and learning reduce the harmfulness of incidents in the long term; thus, the lessons learned should be used to inform future prevention plans.

4.2.5. Integrated Defence-in-Depth and Resource Prioritisation

All protection layers of a system should cooperate with one another, given the different roles that each component undertakes; governance offers form, technology protects systems, human nature influences behaviour, and response strategies provide resilience. According to [16], the priority of entities with limited budgets should be on high-value controls, including access management and employee training. Moreover, Savchenko et al. [7] suggest that metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) can be used to assess effectiveness. In addition, continued review would help ensure that defence mechanisms remain fully updated in the face of changing risks and technologies.

Table 2 shows how each element of the multi-layered mitigation strategy directly responds to the particular risk factors that were identified in Table 1, and a distinct challenge-solution relationship has been established that fully covers insider threat vulnerabilities in the municipal setting. **Figure 2** provides a detailed visual representation of the multi-layered approach to mitigation strategy, which is a combination of governance, technical controls, human factors, and response mechanisms in a defence-in-depth approach to municipal data insider threats.

Table 2. Mapping of risk factors to mitigation strategy components.

Category	Key Risk Factors	Mitigation Layer	Specific Controls
Organisational	Lack of oversight, weak policies, and decentralisation	Governance and policy control	RBAC, insider threat programme, regular access reviews, policy of data classification, and off-boarding.
Human	Disgruntled employees,	Human and Behavioural Controls	Security awareness training, positive security culture programs, whistleblower protection, staff

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

	personal stress, and low morale		security processes, reporting, and mechanisms
Technical	Legacy systems, excessive privileges, and poor logging	Technical and system controls	MFA implementation, PAM systems, SIEM/UEBA monitoring, network segmentation, and end-to-end audit logging.
All Categories	Slow detection and response	Incident Response and Recovery	Insider-specific IR plan, forensic preparedness, continuous improvement process, MTTD/MTTR measures monitoring.

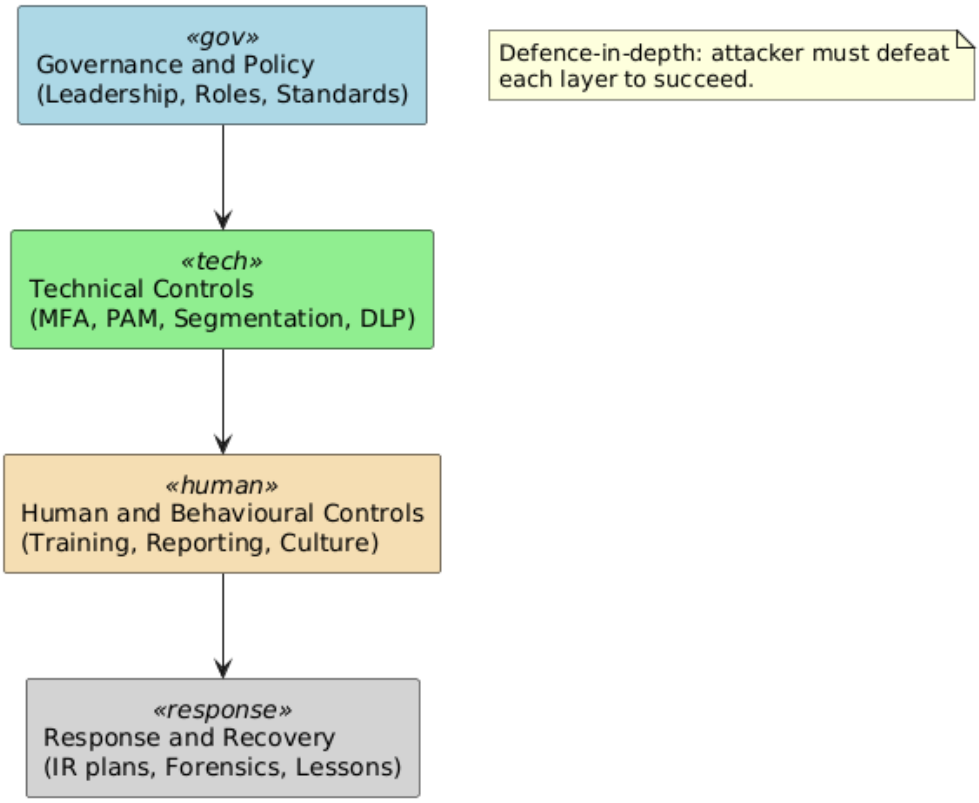

Figure 2. Multi-layered mitigation strategy model.

5. Implementation

5.1. Framework Implementation and Resource Considerations

Implementing an insider threat mitigation strategy on the municipal level requires a resource-sensitive, phased approach, where governance, technology, and human capital are equally balanced. An effective model is grounded in the implementation of original governance mechanisms, such as the formation of a cross-departmental insider threat programme and the establishment of formal risk ownership functions. Supporting this, Chandra et al. [10] found that situational awareness and structured assessment frameworks can be used to improve the decisions made at the initial stages of implementation to identify high-risk data assets and access points.

This implementation may be structured into four stages.

- Phase 1: a foundation aimed at the creation of insider threat policies, training, and awareness.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

- Phase 2: technical integration, involving the implementation of multi-factor authentication, privileged access management, and audit logs to apply principles of least privilege.
- Phase 3: behavioural analytics and automation, involving the implementation of AI-based anomaly detection systems to improve monitoring, which would fit an explainable AI system [13].
- Phase 4: continuous improvement, involving performance audits, lessons learned, and proactive training based on emerging threat intelligence.

Table 3. Implementation phase and key accounts.

Phase	Focus Area	Activities	Expected Outcomes
Foundation	Governance and Policy	Form an insider threat team, develop a policy, and conduct awareness training	Established governance and awareness
Deployment	Technical Controls	Implement MFA, PAM, and DLP tools	Improved access and data control
Monitoring	Analytics and Detection	Monitor activity using SIEM and UEBA	Early detection of malicious behaviours
Improvement	Review and Audit	Conduct audits, policy updates, and staff retraining	Continuous resilience

Given that resource allocation is a significant challenge to municipalities, budgetary limitations can be countered by utilising joint cybersecurity services or federal/state grants. According to [19], the ideas of personnel reliability and specific investment in training are as important as the technology purchased. Economies of scale can also be facilitated in cybersecurity infrastructure through inter-municipal collaboration and through public–private partnerships [20]. In addition, preventive controls can be enhanced with human intelligence elements, including counterintelligence tests performed on critical positions [21]. Lastly, successful implementation can be achieved by matching technical measures to the organisational culture and regularly assessing the programme's maturity.

5.2. Ethical, Legal, and Privacy Considerations

Insider threat mitigation in a municipal setting must resolve security needs with ethical and legal considerations to safeguard the privacy of employees and trust in communities. Strict compliance regimes, including data protection laws, labour controls, and transparency requirements, govern municipalities. Thus, ethical supervision must ensure that monitoring systems do not infringe on privacy at the expense of attaining reasonable security goals. Following [14], the principle of social technical governance insists that insider monitoring must be visible, fair, and accountable in order to avoid depleting employee morale and lowering institutional trust.

5.2.1. Ethical Considerations

Municipalities should develop ethical standards that can strike a balance between security surveillance and the dignity of employees and organisational trust. In a bid to prevent any frustration and isolation, the leaders of the municipalities should increase the levels of fairness, transparency, and openness in the monitoring practices. Ethical supervision should guarantee that the monitoring systems are not used to violate privacy in an attempt to achieve a reasonable security objective [14]. The ethical communication and whistleblower protection frameworks would contribute to the creation of trust and encourage the reporting of suspicious activity in a timely manner [21]. City insider threat programmes need to consider the concepts of fairness, transparency and accountability, and appropriate security strongly depends on long-term trust of the people and the maturity of technical control mechanisms

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

5.2.2. Legal Considerations

Legal risks may arise from the utilisation of behavioural monitoring technologies, insofar as the digital footprints of employees or their communication activities are examined. Alsowail and Al-Shehari [22] state that countermeasure frameworks should be based on direct policy guidelines and informed consent procedures in order to guarantee lawful surveillance. The integration of powerful AI-based detection systems might introduce challenges related to interpretability. According to Islam et al. [13], explainable and interpretable AI is required in cybersecurity decisions to curb algorithmic bias and to avoid due process in investigations.

5.2.3. Privacy Considerations

Local authorities must also adhere to local privacy regulations including GDPR or local privacy regulations by ensuring a balance between the level of monitoring and the level of risk. Based on Figure 3, the municipalities are required to effectively strike a balance between security surveillance and ethical and legal considerations to preserve the privacy of employees so that surveillance efforts are reasonable, transparent, and adherent to the relevant regulations. Ethical communication and whistleblower safeguarding systems would add to the development of trust and motivate timely reporting of suspicious activity [21]. Legally, proper documentation, chain-of-custody procedures, and policies to notify the organisation and individuals would guard against procedural violations [19]. Simply put, the concepts of fairness, transparency, and accountability should be reflected in city insider threat programmes, in which the level of proper security is highly reliant on long-term public trust, as well as on the maturity of technical control measures.

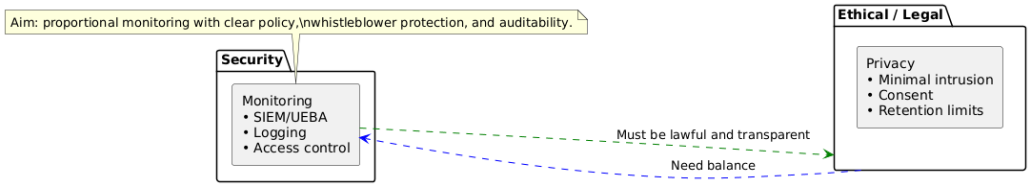

Figure 3. Ethical and legal balance in employee monitoring.

6. Conclusions and Recommendations

The increasing complexity of insider threats poses a significant threat to the security of municipal data. Our research suggests that the mitigation process ought to be holistic and incorporate governance, technical, behavioural, and ethical facets. As municipalities store and process sensitive data about their citizens, they must utilise active, responsive, and intelligence-driven systems of defence. Studies support this, emphasising the importance of encouraging situational awareness, 24 h observation, and a sense of responsibility as keys to insider threat prevention [10,23].

Policy suggestions include institutionalising specific insider threat programmes into the cycles of municipal governance, using ongoing training and employee vetting as a vital element of human resources, and using explainable AI tools to manage risks dynamically [13]. Moreover, interagency partnerships can lead to the sharing of security services and skills between small and mid-sized municipalities with the help of State or federal grants. According to [19,21], introducing human intelligence and counterintelligence factors increases resistance to espionage or politically oriented insider attacks.

Lastly, all insider threat strategies should consider ethical and privacy-related issues. Oversight transparency, accurate data use policies, and a continuous discussion of privacy implications are a means of building employee and citizen trust. Future studies should discuss the patterns of predictive models in low-resource municipal settings, and comparative studies should be performed on the framework of insider threats as they exist in different jurisdictions. Municipality leaders must also understand that insider threat reduction is not only a technical procedure but also a foundation of democratic data custodianship and robust citizen administration.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

Author Contributions: Conceptualization, S.T.T. and S.A.S.; methodology, S.T.T.; formal analysis, S.T.T.; investigation, S.T.T. and S.A.S.; writing—original draft preparation, S.T.T.; writing—review and editing, S.T.T. and S.A.S.; visualization, S.T.T.; supervision, S.A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Data Availability Statement: No new data were created or analysed in this study. This paper presents a theoretical framework based on existing literature. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Inayat, U.; Farzan, M.; Mahmood, S.; Zia, M.F.; Hussain, S.; Pallonetto, F. Insider threat mitigation: Systematic literature review. *Ain Shams Eng. J.* **2024**, *15*, 103068. https://doi.org/10.1016/j.asej.2024.103068.
2. Akinsola, F.A.; Ogwueleka, F.N.; Mbanaso, U.M. A Comprehensive Survey of Insider Threat Landscape and Detection Indicators. *Int. J. Eng. Inf. Technol.* **2025**, *2*, 146–177. https://doi.org/10.58578/kijeit.v2i3.7704.
3. Alsowail, R.A.; Al-Shehari, T. A Multi-Tiered Framework for insider threat prevention. *Electronics* **2021**, *10*, 1005. https://doi.org/10.3390/electronics10091005.
4. Steinmetz, M. The 'Insider Threat' and the 'Insider Advocate. In *The Oxford Handbook of Cyber Security*; Oxford University Press: Oxford, UK, 2021; pp. 348–358. https://doi.org/10.1093/oxfordhb/9780198800682.013.21.
5. Vestad, A.; Yang, B. Municipal Cybersecurity—A neglected research Area? A survey of current research. In Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social MediaCyber Science 2022, Wales, UK, 20–21 June 2022; Springer Proceedings in Complexity; Springer: Singapore, 2023, pp. 151–165. https://doi.org/10.1007/978-981-19-6414-5_9.
6. Safa, N.S.; Abroshan, H. The effect of organizational factors on the mitigation of information security insider threats. *Information* **2025**, *16*, 538. https://doi.org/10.3390/info16070538.
7. Savchenko, V.; Dzyuba, T.; Matsko, O.; Novikova, I.; Havryliuk, I.; Polovenko, V. Time aspect of insider threat mitigation. *Adv. Mil. Technol.* **2024**, *19*, 149–164. https://doi.org/10.3849/aimt.01830.
8. Nagel, K.; CISA; CRISC; CISSP. Establishing a Foundation and Building an Insider Threat Program. *ISACA J.* **2021**, *5*, 1–7. Available online: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/establishing-a-foundation-and-building-an-insider-threat-program (accessed on 29 October 2025).
9. Cornelius, F.P.; Van Rensburg, S.K.J. Emerging South African smart cities: Data security and privacy risks and challenges. *S. Afr. J. Inf. Manag.* **2024**, *26*, 11. https://doi.org/10.4102/sajim.v26i1.1847.
10. Chandra, N.A.; Ramli, K.; Ratna, A.A.P.; Gunawan, T.S. Information security risk assessment using situational awareness frameworks and application tools. *Risks* **2022**, *10*, 165. https://doi.org/10.3390/risks10080165.
11. Zeng, M.; Dian, C.; Wei, Y. Risk assessment of insider threats based on IHFACS-BN. *Sustainability* **2022**, *15*, 491. https://doi.org/10.3390/su15010491.
12. Al-Mhiqani, M.N.; Ahmad, R.; Abidin, Z.Z.; Yassin, W.; Hassan, A.; Abdulkareem, K.H.; Ali, N.S.; Yunos, Z. A review of insider threat detection: classification, machine learning techniques, datasets, open challenges, and recommendations. *Appl. Sci.* **2020**, *10*, 5208. https://doi.org/10.3390/app10155208.
13. Islam, S.; Basheer, N.; Papastergiou, S.; Ciampi, M.; Silvestri, S. Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. *J. Reliab. Intell. Environ.* **2025**, *11*, 12. https://doi.org/10.1007/s40860-025-00253-3.
14. Lishchynsky, M. The Insider Threat: A Socio-Technical Analysis of Preventing Data Breaches and Espionage Within Governmental Agencies. *Politics Secur.* **2025**, *12*, 88–103. https://doi.org/10.54658/ps.28153324.2025.12.2.pp.88-103.
15. NIST. *Security and Privacy Controls for Information Systems and Organisations*; NIST Special Publication 800-53; National Institute of Standards and Technology, U.S. Department of Commerce: Washington, DC, USA, 2020. https://doi.org/10.6028/nist.sp.800-53r5.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2025 doi:10.20944/preprints202511.1091.v1

16. Sektas-Bilusich, D.; Nunes-Vaz, R.A.; Chim, L.; Lord, S. A Risk-Based framework to inform prioritisation of security investment for insider threats. *Int. J. Saf. Secur. Eng.* **2020**, *10*, 49–57. https://doi.org/10.18280/ijsse.100107.
17. Gheyas, I.A.; Abdallah, A.E. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Anal.* **2016**, *1*, 6. https://doi.org/10.1186/s41044-016-0006-0.
18. Ismail, W.B.W.; Widyarto, S. A classification of human error factors in unintentional insider threats. In Proceedings of the International Conference on Sustainable Practices, Development and Urbanisation (IConsPADU 2021), Virtual, 16 November 2021; Volume 3, pp. 667–676. https://doi.org/10.15405/epms.2022.10.63.
19. Rajagopalan, R.P.; Lynch, P.; Burbach, T. Mitigating insider threats and ensuring personnel reliability. In *The Challenges of Nuclear Security*; Palgrave Macmillan: Cham, Switzerland, 2024; pp. 29–69. https://doi.org/10.1007/978-3-031-56814-5_2.
20. Whitty, M.T. Developing a conceptual model for insider threat. *J. Manag. Organ.* **2018**, *27*, 911–929. https://doi.org/10.1017/jmo.2018.57.
21. Kanellopoulos, A.-N. Insider threat mitigation through human intelligence and counterintelligence: A case study in the shipping industry. *Def. Secur. Stud.* **2024**, *5*, 10–19. https://doi.org/10.37868/dss.v5.id261.
22. Alsowail, R.A.; Al-Shehari, T. Techniques and countermeasures for preventing insider threats. *PeerJ Comput. Sci.* **2022**, *8*, e938. https://doi.org/10.7717/peerj-cs.938.
23. Saxena, N.; Hayes, E.; Bertino, E.; Ojo, P.; Choo, K.-K.R.; Burnap, P. Impact and key challenges of insider threats on organisations and critical businesses. *Electronics* **2020**, *9*, 1460. https://doi.org/10.3390/electronics9091460.
24. National Whistleblower Center (NWC). The Fraud Triangle: A Model for Identifying High Risks of Fraud Highlights Three Factors That Lead to Fraud: Motivation, Opportunity, and Rationalisation. National Whistleblower Center: Washington, DC, USA, [online] 2023. Available at: https://www.whistleblowers.org/fraud-triangle/(accessed on 5 November 2025).
25. EverEdge Global. Preventing Disloyal MICE in the Company Floorboards. EverEdge Global News: 7 September 2023. Available at: https://www.everedgeglobal.com/news/preventing-disloyal-mice-in-the-company-floorboards/(accessed on 5 November 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.