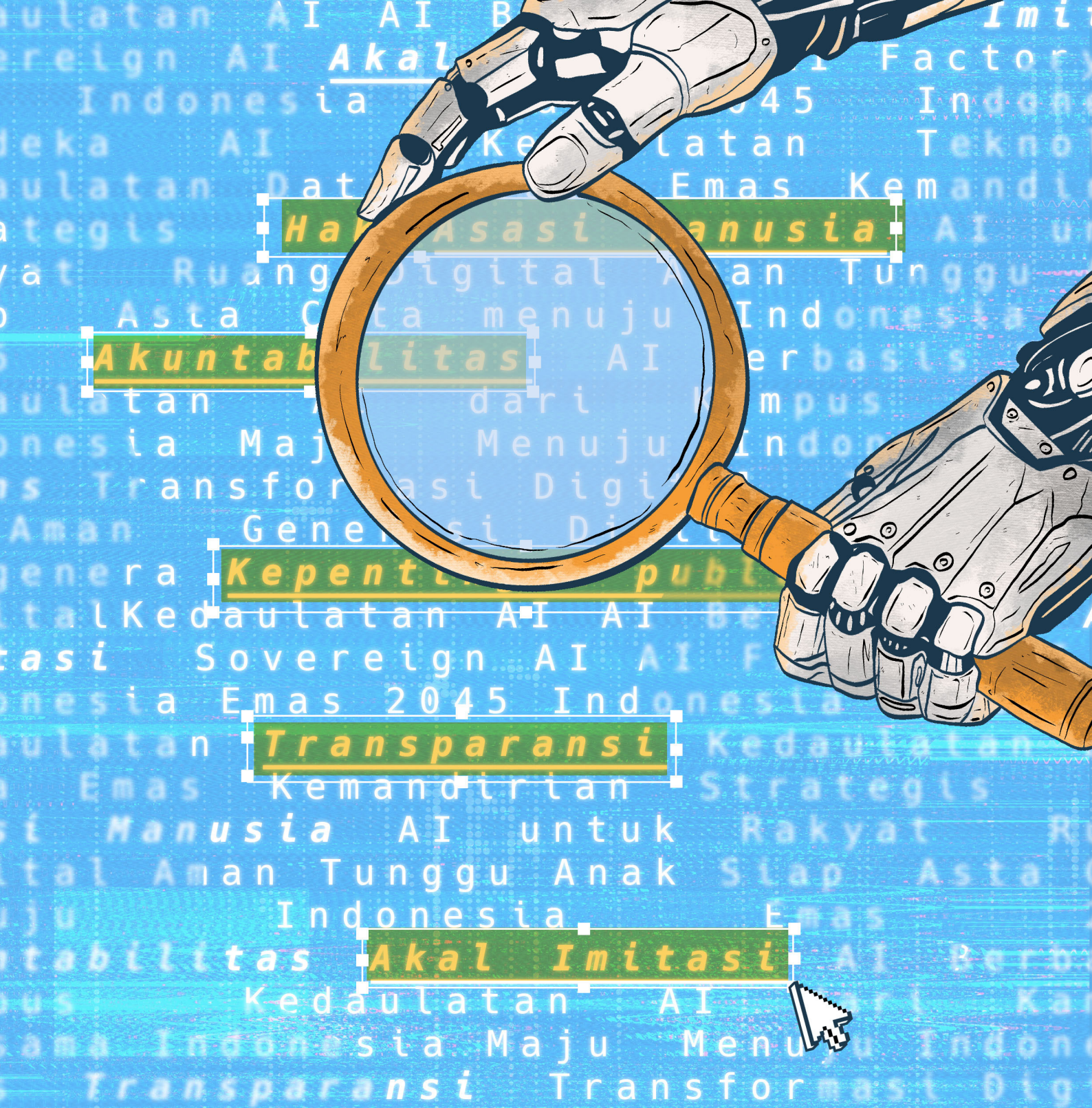




Strategic Recommendations: Strengthening *National Digital Sovereignty* through *Human Rights-Based AI Incident Reporting*

Executive Summary

[The Indonesian Minister for Communications and Digital Affairs](#), Meutya Hafid, stated in a speech in February 2026 that the value of the national digital economy had exceeded USD80 billion and was projected to surpass USD130 billion by 2025. This vision and ambition to become an AI innovation hub in ASEAN also drives the Indonesian government's efforts to achieve sovereignty in artificial intelligence (hereinafter referred to as AI) by developing an AI ecosystem [through the flagship AI Talent Factory Programme](#). This supports [President Prabowo's goals for 2024–2029](#), particularly the fourth point of the *Asta Cita*, which emphasises the need to improve the skills of approximately [12 million digital talents](#) to achieve Indonesia's control over technology while ensuring the well-being of all Indonesians—from those who create technology to those who use it—within an AI system that respects human rights, allowing technological progress in all areas to thrive and potentially make Indonesia the largest in Southeast Asia.

As a logical consequence, the Ministry of Communication and Digital Transformation is now developing the implementing regulations for the Draft Presidential Regulation on Digital Ethics while keeping human rights in mind. In a position paper drafted by Ramzy M. ([SAFE-net](#)) with contributions from our colleagues Alia Yofira ([PurpleCode Collective](#)), Chikita Edrini Marpaung ([LBH Pers](#)), Karlina Octaviany ([GIZ-Fair Forward](#)), Shita Laksmi (independent), and [EngageMedia](#), we recommend two key points as input for the formulation of the AI incident reporting framework, namely the following:

1.

Users and the general public can report or complain about AI incidents. These include people who utilise the AI system directly through a user interface or AI services provided by sectoral actors, as well as anyone who is directly or indirectly impacted by the AI life cycle.

2.

A mandatory reporting system must include:

- a. Retention of audit records & documentations to track the progress of an incident report.
- b. The AI system must be reviewed by a person who makes the final decision. Sectoral actors may only use the AI system's output as the basis for a decision if it has legal consequences or a significant impact on human rights, life, livelihoods or the welfare of any individual.
- c. A chain of responsibility for recovery/redress in the event of negligence as well as when the system directly or indirectly causes harm and/or violates human rights.

These proposed improvements follow [the Civil Society Position Paper “Breaking Barriers: Centring Human Rights in the National AI Strategy Towards #GoldenIndonesia2045”](#) (July 2025), as well as feedback [from civil society groups during the public consultation on the draft Presidential Regulation on AI Ethical Guidelines and the other draft Presidential Regulation](#).

These recommendations stem from concerns about the AI’s persistent impact on the local community¹. From 2022 to the present, media monitoring of the impact of AI ([MMAAI](#)) has recorded at least [123 incidents, with at minimum 162 identifiable individuals harmed by incidents that appear to have been enabled by AI](#). The parties involved come from all sectors related to the AI’s entire lifecycle, making the public a crucial part of the incident reporting system.

One example of the impact of data centres on people’s livelihoods can be seen in the experiences of Batam’s residents. Drought and water shortages, according to [reports from residents](#), have occurred in tandem with the construction of 18 data centres in the Batam Industrial Complex. By 2024, water will flow for only a few hours a day in residential areas, whilst the industrial complex will have continuous water flow. When fully operational in 2032, 10 data centres are estimated to consume [8 per cent of the total](#) water supply currently available, or the equivalent of the needs of a quarter of Batam’s population.

Most worryingly, children’s personal data has also been compromised. In February 2026, profile data on parents, Google Maps locations and physical conditions of [58 million Indonesian pupils were reportedly leaked](#) and were being traded freely on the DarkForums hacker forum. The leak is strongly suspected to have stemmed from a security breach within the Basic Education Data digital ecosystem.

Ideally, incident reporting should adopt an evidence-based, multidimensional and life-cycle-orientated approach to monitoring AI incidents. This is not intended to undermine or slow down innovation, but rather to establish a systematic method for answering seven interrelated questions:

What happened? → Did AI play a part? → Why did it happen? → What AI risks does this represent? → What are the consequences? → How severe and how widespread are these consequences? → Who is responsible or in control?

These questions converge towards a single ultimate goal: to create a credible evidence base in the public interest and as a learning tool for the private sector and policymakers, enabling comparisons of incidents across sectors, jurisdictions, technologies and times.

¹The public, in this context, forms part of the user group, namely any person who uses an AI system directly via a user interface or an AI-based service provided by a sector actor, or any person who is directly or indirectly affected by the AI life cycle.

Proposed Changes and/or Additions from Civil Society Groups for Reporting AI Incidents

Specific articles of concern

Chapter I (General Provisions)

Draft Article	Recommendations for Alternative Provisions	References
Article 1, point X Ministries or Agencies, hereinafter referred to as Ministries/ Agencies, are legislative, executive and judicial institutions at central and regional levels, as well as other bodies established by law, which are responsible for supervising and issuing regulations governing their respective sectors.	Article 1, point X A public body is an executive, legislative or judicial institution, and other bodies whose primary functions and duties relate to the administration of the state, where some or all of their funding is derived from the State Revenue and Expenditure Budget and/or the Regional Revenue and Expenditure Budget, or non-governmental organisations provided that some or all of their funding is derived from the State Revenue and Expenditure Budget and/or the Regional Revenue and Expenditure Budget, public donations, and/or foreign sources.	

Draft Article	Recommendations for Alternative Provisions	References
<p>Article 1, point X</p> <p>AI ethics is a set of moral principles that provide a foundation to ensure the development, implementation, and use of AI are carried out responsibly, fairly, and transparently, while respecting privacy, ensuring security, allowing human oversight, and complying with applicable legal provisions.</p>	<p>Article 1, point X</p> <p>Artificial Intelligence Ethics are moral principles that serve as a foundation to ensure that the processes of design, development, testing, use, maintenance, decommissioning and procurement of AI support infrastructure are based on established ethical values.</p>	
<p>Article 1, point X</p> <p>[UNKNOWN]</p>	<p>Article 1, point X</p> <p>The Artificial Intelligence Life Cycle comprises the entire process of the design, development, testing, use, maintenance, decommissioning and procurement of infrastructure supporting AI.</p>	
<p>Article 1, point X</p> <p>[UNKNOWN]</p>	<p>Article 1, point X</p> <p>'Sectoral Actors' means any person, public body or international organisation involved in any and/or all processes of the AI life cycle, whether within or outside the jurisdiction of the Republic of Indonesia.</p>	<p><i>The definition of "person" refers to Article 1 of the ITE Law (No. 11 of 2008, as amended by No. 19 of 2016 and No. 1 of 2024) and Article 1 of Government Regulation No. 71 of 2019: "21. A person means an individual, whether an Indonesian citizen, a foreign national or a legal entity."</i></p>

Draft Article	Recommendations for Alternative Provisions	References
<p>Article 1, point X</p> <p>[UNKNOWN]</p>	<p>Article 1, point X</p> <p>An Artificial Intelligence Incident, hereinafter referred to as an AI Incident, is an event occurring during or as a result of the AI life cycle which, directly or indirectly, causes harm and/or infringes human rights in accordance with the provisions of legislation.</p> <p>Explanation (if necessary): The harm caused and/or human rights infringements in accordance with the provisions of legislation may take the form of:</p> <ul style="list-style-type: none"> a. harm to a person's health or safety; b. violations of human rights, including the right to privacy and the protection of personal data, freedom of expression, the right to be free from discriminatory treatment, and the right to be free from electronic-based sexual violence as referred to in legislation concerning criminal offences of sexual violence; c. violations of workers' rights or the rights of individuals who earn an income through the electronic system; d. disruption to the provision of public services or vital infrastructure; e. harms to economic interests or to property suffered by Users and/or the Public; f. environmental damage or harm to the Public; and/or g. Technology-Facilitated Gender-Based Violence (TFGBV) against a person, particularly women, children, people with disabilities, indigenous peoples, and/or other vulnerable groups. 	

Draft Article	Recommendations for Alternative Provisions	References
Article 1, point X [UNKNOWN]	<p>Article 1, point X</p> <p>A Serious AI Incident is an AI incident that results in a violation of fundamental human rights which cannot be mitigated under any circumstances in accordance with the provisions of legislation.</p> <p>Explanation (if necessary):</p> <p>Fundamental human rights violations that cannot be mitigated under any circumstances, in accordance with the provisions of legislation, may include:</p> <ul style="list-style-type: none"> a. loss of life or serious or irreversible harm to health; b. widespread disruption to vital infrastructure or public services; c. serious or irreparable human rights violations; and/or d. systemic harms or harms suffered by a large number of Users and/or the Public. 	
Article 1, point X A 'User' means an end-user, namely a party who uses an AI system directly via a user interface or an AI-based service.	<p>Article 1, point X</p> <p>A 'User' means any person who uses an AI system directly via a User interface or an AI-based service provided by a Sector Operator, or any person who is directly or indirectly affected by the AI life cycle.</p> <p><i>The definition of "person" refers to Article 1 of the ITE Law (No. 11 of 2008, as amended by No. 19 of 2016 and No. 1 of 2024) and Article 1 of Government Regulation No. 71 of 2019: "21. A person means an individual, whether an Indonesian citizen, a foreign national or a legal entity."</i></p>	
Article 1, point X Addition of a new article	<p>The Public is defined as a group of Individuals, both legal and natural persons, with a direct or indirect interest in the AI life cycle.</p>	

Chapter X (Artificial Intelligence Systems)

Draft Article	Recommendations for Alternative Provisions	References
New Article – Oversight Mechanisms in AI Decisions	<ol style="list-style-type: none"> 1. The output of an AI system may only form part of the basis for a decision by a Sector Actor if it gives rise to legal consequences or has a significant impact on the human rights, life, livelihood or well-being of any Person. 2. The decisions referred to in paragraph (1) include decisions concerning: <ol style="list-style-type: none"> a. the termination, suspension or restriction of any Person's access to services; b. the setting of tariffs, the allocation of work, performance appraisals, and the imposition of sanctions on individuals who derive income through the electronic system; c. access to public services, including healthcare, education and financial services; and d. the enforcement of terms of service against any Person using such services. 3. Every Person is entitled to request a review by a human of the decision referred to in paragraph (1). 4. Sector Operators must appoint an authorised and competent individual with the power to amend or revoke the decision to carry out the review referred to in paragraph (3). 5. Sector Operators shall communicate the results of the review to Users in writing, together with the reasons, no later than 14 (fourteen) calendar days from receipt of the request for review. 	<ul style="list-style-type: none"> • GDPR Article 22(3) • EU AI Act Article 86, • Platform Work Directive (EU) 2024/2831 Articles 7 & 8.

Draft Article	Recommendations for Alternative Provisions	References
	<p>6. Sector Operators shall provide an explanation of the decision referred to in paragraph (1) to Users free of charge and in a language that is easy to understand, which shall include at least:</p> <ol style="list-style-type: none"> information that the decision was made using an AI system; the types of data relating to the User that were used; 	
	<ol style="list-style-type: none"> the main factors influencing the decision; and the procedure for requesting a review as referred to in paragraph (3). <p>7. The requirement for human review applies to content moderation decisions generated by an AI system, including the removal of content, account suspensions and closures, in accordance with the self-regulatory content moderation provisions set out in the government regulation on the operation of electronic systems and transactions.</p>	
<p>New clause – Retention of AI system records</p>	<ol style="list-style-type: none"> Sector Operators are required to retain a record of the operation of the AI system for a minimum of 5 (five) years, which must include at least the following: <ol style="list-style-type: none"> the time of the event input output the version of the model used, and the identity of the party carrying out the supervision. In the event of a report of an AI incident, the Sector Operator shall provide the relevant records to the Director-General and to the reporting party, provided that such records do not contain the personal data of other parties. The Director-General and the Sector Operator shall continue to follow up on reports of AI incidents even if the record referred to in paragraph (1) is not available. 	<ul style="list-style-type: none"> EU AI Act Articles 12 & 19 Korea's AI Framework Act Article 34

Chapter X (AI Incident Reporting System)

Draft Article	Recommendations for Alternative Provisions	References
<p>Article X – AI Incident Reporting System</p> <ol style="list-style-type: none"> 1. Users may submit reports of complaints and/or incidents of breaches of the Code of Ethics for AI to the Director-General and/or directly to the Electronic System Operator, which is the AI System Operator. 2. The reports referred to in paragraph (1) must include, as a minimum, the following administrative documents: <ol style="list-style-type: none"> a. Identity of the complainant; b. Identity of the Electronic System Operator as the party against whom the complaint is made; c. Description of the complaint and/or incident; and d. Supporting evidence for the complaint and/or incident. 	<p>Article X</p> <ol style="list-style-type: none"> 1. Sector Operators are required to establish a reporting system for AI incidents that occur during or as a result of the AI life cycle, as part of their obligation to protect all Individuals from harms caused by the AI systems they operate. 2. Sector Operators are required to establish an incident reporting system that: <ol style="list-style-type: none"> a. accessible to the public; b. secure, reliable and sustainable; c. prioritises the interests of every affected person; d. contains information on mechanisms or procedures for direct, indirect and/or electronic reporting that is easily accessible and understandable; e. is accessible free of charge; f. is available in Indonesian; g. is screen-reader compatible; and h. provides non-electronic channels for Users who do not have electronic access. 3. Any Person, Group, Community or Organisation directly or indirectly affected by the operation of an AI system or by a decision made by an AI system is entitled to submit a report regarding any incident that does not comply with the obligations set out in these regulations. 4. Any Person may submit a report as referred to in paragraph (3) either independently or through a body established by the Public 	<ul style="list-style-type: none"> • Article 31 of Government Regulation No. 71/2019 • Article 3 paragraph (2) of Government Regulation No. 76/2013 • Articles 41 paragraphs (2) and (3) of the ITE Law

Draft Article	Recommendations for Alternative Provisions	References
	<p>as referred to in the legislation concerning electronic information and transactions.</p> <p>5. The report referred to in paragraph (3) must be accompanied by at least:</p> <ol style="list-style-type: none"> Identity of the complainant; Identity of the Sector Operator as the respondent; Description of the incident; and Supporting evidence relating to the incident. <p>6. Sector Operators and Directors-General are obliged to keep the identity of the complainant confidential from the reported party, unless the complainant provides their written consent.</p> <p>7. In the management of the incident reporting system, Sector Operators are obliged to:</p> <ol style="list-style-type: none"> announce the name and office address of the person responsible for managing the incident reporting system; communicate the mechanisms and procedures for managing incident reporting; receive, respond to, process and resolve every incident report; forward incident reports that fall outside its remit to the relevant authority; to record and report on the management of incident reports; and to monitor and evaluate the management of incident reporting. 	

Draft Article	Recommendations for Alternative Provisions	References
	<p>8. Records of each AI incident report must include at least the following:</p> <ul style="list-style-type: none"> a. report identification number; b. description of the AI incident; c. date of the AI incident; d. location of the AI incident; e. sector of application, including its connection to critical infrastructure; f. responsible parties, including developers, providers and operators of the AI system; g. a description of the AI system, including its functions, the techniques used, the level of autonomy, User characteristics and the type of input data; h. a description of the resulting impacts, their causes where known, and their subsequent consequences; i. provisions of legislation that may have been breached; j. immediate response measures taken; k. corrective and preventative actions, such as reviewing the impact assessment to ensure compliance with applicable regulations; and l. the party receiving the follow-up to the report and the timeframe for such follow-up. <p>9. Sector Operators are prohibited from ceasing, suspending, restricting or discriminating against a complainant on the grounds that the complainant has submitted a report of an AI incident that does not fall within the remit of a specific Ministry or Agency and/or that the reported AI incident is suspected not to be an incident.</p>	

Draft Article	Recommendations for Alternative Provisions	References
New Article – Reporting Periods and Mechanisms	<p>Article X</p> <ol style="list-style-type: none"> 1. When handling reports of AI incidents, Sector Operators must: <ol style="list-style-type: none"> a. issue a receipt to the complainant no later than 1x24 (one times twenty-four) hours after receiving the complaint; b. respond substantively to the complaint no later than 10 (ten) working days after receiving it; c. resolve the complaint no later than 30 (thirty) calendar days after receiving the complaint. 2. Sector Operators may extend the time limit referred to in paragraph (1) (c) once, for a maximum of 30 (thirty) calendar days, and must notify the reporter in writing of the reasons for the extension. 3. The Director-General shall respond to the report within 10 (ten) working days at the latest and shall complete the processing of the report within 60 (sixty) calendar days at the latest from the date of receipt. 	Art 73 EU AI Act
New Article – Reporting of Serious AI Incidents	<p>Article X</p> <ol style="list-style-type: none"> 1. Sector Operators are required to report any Serious AI Incident to the Director-General no later than 3x24 (three times twenty-four) hours after becoming aware of the Serious AI Incident, without waiting for a report. 2. Where information regarding a Serious AI Incident is incomplete, the Sector Operator shall submit an initial report within the timeframe referred to in paragraph (1) and shall complete the report no later than 14 (fourteen) calendar days from the date of submitting the initial report. 	

Draft Article	Recommendations for Alternative Provisions	References
<p>New Article – Incident Reporting Mechanism</p>	<p>Article X</p> <ol style="list-style-type: none"> 1. The reporting system for AI incidents arising from the operation of AI systems by the Sector Operators shall be administered by the Director-General. 2. With regard to the incident reports referred to in paragraph (1), the Director-General shall: <ol style="list-style-type: none"> a. provide a response to the report to the reporting party; b. conduct an independent investigation into the report and/or request verification of the report from the relevant Sector Operator; c. notify Users regarding reports concerning the operation of an AI system by a Sector Operator; and d. reject the report if the operation of the AI system by the Sector Operator in question does not constitute an incident. 3. The Director-General shall notify the complainant in writing of the rejection of the report as referred to in paragraph (2) (d), stating the reasons therefore. 4. The complainant may lodge an objection to the rejection as referred to in paragraph (3) with the Minister no later than 14 (fourteen) calendar days from receipt of the rejection. 5. A summary and/or analysis of incidents arising from the operation of an AI system by a Sector Operator shall constitute public information provided that it does not contain specific personal data as regulated by the provisions of legislation on the protection of personal data. 6. In the event that the Sector Operator is a Public Company as regulated by the provisions of legislation: <ol style="list-style-type: none"> a. A summary and/or analysis of incidents arising from the operation of an AI system by a Sector Operator shall not be regarded as a trade secret, provided that it does not contain specific personal data as stipulated by the provisions of legislation on the protection of personal data. 	

Draft Article	Recommendations for Alternative Provisions	References
	<p>b. Summaries and/or analyses of incidents arising from the operation of AI systems by the Sector Operators shall be submitted by the Board of Directors to the Board of Commissioners as part of the annual report, namely the report on the company's activities, provided that they do not contain specific personal data as regulated by the provisions of legislation on the protection of personal data.</p>	
New Article – Enforcement and Liability	<p>Article X</p> <ol style="list-style-type: none"> 1. Where an AI incident report is substantiated, the Sector Operator shall: <ol style="list-style-type: none"> a. to halt or rectify any processes, functions or outputs of the AI system that give rise to an AI incident; b. to revoke or correct decisions resulting from an AI incident and restore the status of the affected User; c. to notify the complainant of the corrective measures, and other affected Users in the event of a Serious AI Incident; and d. to record the measures referred to in points (a) to (c) and report them to the Director-General. 2. The obligation set out in paragraph (1) shall be fulfilled no later than 90 (ninety) calendar days from the date on which the AI incident report is confirmed. 	
New Article – Value Chain	<p>Article X</p> <ol style="list-style-type: none"> 1. Where an AI incident arises from a model or component supplied by a third party, the Sector Operator shall: <ol style="list-style-type: none"> a. include the identity of the supplier of the model or component in the notes to the AI incident report; b. forward the AI incident report to the supplier of the model or component; and c. notify the Director-General and the complainant of the follow-up action referred to in point (b). 	

Draft Article	Recommendations for Alternative Provisions	References
	<ol style="list-style-type: none"> 2. The follow-up to the report referred to in paragraph (1) does not relieve Sector Operators of their obligations under this regulation. 3. The disclosure obligation referred to in paragraph (1) shall remain in force even if records relating to a specific AI incident are classified as exempt information in accordance with the provisions of legislation on public information disclosure. 	
<p>New Article – Publication of the Annual Report</p>	<p>Article X</p> <ol style="list-style-type: none"> 1. The Director-General shall publish a report on the operation of the AI incident reporting system at least once a year, which shall include, as a minimum: <ol style="list-style-type: none"> a. the number of AI incident reports received, followed up on, rejected and resolved; b. categories of AI incidents; c. the relevant sectors and types of AI systems; d. the time taken to resolve reports; and e. corrective actions taken by Sector Operators. 2. The Director-General shall publish the report referred to in paragraph (1) in an open, machine-readable format and without including any specific personal data, as provided for in the provisions of the legislation on the protection of personal data. <p>Proposed explanation: The AI incident reporting data referred to in Article X shall be published in a format that is interoperable with publicly managed incident databases.</p>	

Draft Article	Recommendations for Alternative Provisions	References
New Article – Inter-agency Coordination	<p>Article X</p> <p>Where the handling of an AI incident falls within the remit of another Ministry or Agency, the Director-General shall follow up on the report with that Ministry or Agency no later than 7 (seven) working days from receipt of the report and shall inform the complainant of such follow-up.</p> <p>Article X</p> <p>Where an AI incident also constitutes a personal data breach, the Sector Operator shall fulfil its notification obligations under the legislation on personal data protection in addition to the obligations set out in these regulations.</p> <p>Article X</p> <ol style="list-style-type: none"> 1. The obligation to report AI incidents under these regulations applies separately from, and does not replace, the obligation to report cybersecurity incidents under legislation concerning cybersecurity and resilience. 2. Where an AI incident also constitutes a cybersecurity incident, the Sector Operator shall submit both reports in accordance with the provisions, and the Director-General shall coordinate with the competent authorities in the field of cybersecurity. <p>Article X</p> <p>When handling reports of AI incidents involving online sexual violence against any person, particularly women, children, persons with disabilities, indigenous peoples or other vulnerable groups, Sector Operators and the Director-General shall take into account the needs, safety and confidentiality of the victims and shall forward the reports to the competent authorities in accordance with the applicable laws and regulations.</p>	

Draft Article	Recommendations for Alternative Provisions	References
New Article – Recovery and Accountability Mechanism	<p data-bbox="416 237 533 271">Article X</p> <ol style="list-style-type: none"> <li data-bbox="440 320 1145 790">1. Any Person who has suffered harm as a result of the operation of an AI system by a Sector Operator may bring a claim in accordance with the laws and regulations concerning electronic information and transactions in the following circumstances: <ol style="list-style-type: none"> <li data-bbox="491 555 1094 633">a. reports of AI incidents are not followed up properly, adequately and/or fairly; or <li data-bbox="491 633 1094 790">b. an Electronic System Operator which is also an AI System Operator neglects its obligations and/or contravenes the prohibitions set out in these regulations. <li data-bbox="440 790 1145 1032">2. Where summaries and/or analyses of AI incidents are classified as information subject to unilateral exemption, any person may lodge an objection or bring a dispute concerning public information in accordance with the laws and regulations on public information disclosure. <li data-bbox="440 1032 1145 1227">3. The legal action referred to in paragraph (1) may take the form of a civil claim, a class action brought by the public, or alternative dispute resolution, in accordance with the applicable rules of procedure. <li data-bbox="440 1227 1145 1429">4. The use of the AI incident reporting system referred to in Article X shall not constitute a prerequisite for bringing a legal action, raising an objection, lodging a complaint, or taking any other legal action. 	

ulatan AI AI Berdaula Akal Imitasi
reign AI Akal Imitasi AI Factory
Indonesia Emas 2045 Indonesia
eka AI Kedaulatan Tekno
ulatan Data Data Emas Kemandi
tegis Hak Asasi Manusia AI un
at Ruang Digital Aman Tunggu
Asta Cita menuju Indonesia
Akuntabilitas AI Berbasis Ka
ulatan AI dari Kampus Ber
nesia Maju Menuju Indonesia
s Transformasi Digital Tata Ke
Aman Generasi Digital Masa De
enera Kepentingan publik Ekosi
talKedaulatan AI AI Berdaulat
asi Sovereign AI AI Factory AI
nesia Emas 2045 Indonesia Merdeka
ulatan Transparansi Kedaulatan
Emas Kemandirian Strategis
i Manusia AI untuk Rakyat Ri
tal Aman Tunggu Anak Siap Asta
ju Indonesia Emas
tabilitas Akal Imitasi AI Berda
us Kedaulatan AI dari Ka
ama Indonesia Maju Menuju Indon
Transparansi Transformasi Dig