

Responsible AI Program 2025



Content

1. Limiting access to sensitive AI capabilities (e.g. facial recognition, surveillance)	7–9
2. Distinct labeling of AI-generated content and outcomes of AI-driven decisions	11–13
3. Mechanisms to detect and correct drift or degradation of AI models over time	15–16
4. Regular assessments of deployed AI models for fairness/bias	17–19
5. Initiatives (own/with suppliers) to lower the ecological footprint of AI data centers/models	20–21
6. Appeals process for users/affected third parties to contest an AI decision or outcome	23–24
7. Quantification of the impact of AI initiatives/tools on sustainability outcomes	26–28
8. Training of employees on the ethical use and/or security of AI	29–35
9. The AI management system verified (e.g. ISO42001)	36–37

Introduction of GPSC's Responsible Artificial Intelligence

As the power and smart-energy flagship of PTT Group, GPSC is bringing Artificial Intelligence (AI) and Generative AI into everyday work from predicting equipment failures and improving plant reliability to supporting corporate decisions, while keeping the company on course toward Carbon Neutrality and Net Zero. We recognize that these tools also introduce new risks around data privacy, cybersecurity, bias, transparency and reliability, and we manage them accordingly.

Our approach rests on four pillars set out in GPSC's AI Governance Guideline: AI Governance; Robustness and AI Security; Transparency and Explainability; and Fairness and Stakeholder Protection. Controls are applied in proportion to risk – the greater a use case's potential impact on people, the power system or the environment, the tighter the controls. The Guideline is written with reference to recognized standards, including ISO/IEC 42001:2023, the NIST AI Risk Management Framework, ISO/IEC 23894, ETDA's Generative AI guidance and Thailand's PDPA, and is connected to the Group's Enterprise Risk Management framework and the Three Lines of Defense model.

In practice, this direction is supported by a company Generative AI usage policy with clear Do's and Don'ts, the enterprise assistant with Microsoft Copilot Studio, a company-wide capability programme (the AI Value Realization Program, "AIVA", together with the AI Bootcamp), and a firm rule that a person always reviews AI output before it is used – captured in the internal principle "AI is an assistant, not a judge."

GPSC AI GOVERNANCE in ACTION

Safe and Effective Use of Generative AI in Organizations

Enterprise Generative AI : Using AI to Drive Organizational Development



- ✓ Use AI to analyze information, summarize content, and create reports.
- ✓ Use AI to improve efficiency and reduce working time.
- ✓ Verify AI-generated outputs before using them in actual work.
- ✓ Report any AI-related issues or risks to the IT department
- ✗ Do not use AI-generated outputs without verifying the information first.
- ✗ Do not input personal data or confidential information into AI systems.
- ✗ Do not use AI to create false, misleading, or illegal content.



“AI is an Assistant, not a judge” Use it responsibly, everyone benefits

GPSC AI GOVERNANCE in ACTION

Safe and Effective Use of Generative AI in Organizations

Personal Generative AI : Use with Caution

Today, generative AI plays an increasingly important role in many areas. Public AI tools such as ChatGPT, Perplexity, Gemini, and DeepSeek each offer unique capabilities, but they should be used responsibly and with appropriate caution.

-  Use AI to help generate ideas and support brainstorming.
-  Use AI to search for and summarize information from public sources.
-  Verify data ownership, copyright, or usage rights before using AI-generated or sourced content
-  Check the credibility and reliability of information sources before relying on AI-generated outputs.
-  Do not use your company account to register for or access public AI services (e.g., ChatGPT, Gemini).
-  Do not upload confidential company information or personal data to public AI platforms.
-  Do not use AI to create unethical, misleading, or inappropriate content.



“AI is an Assistant, not a judge” Use it responsibly, everyone benefits

1. Limiting access to sensitive AI capabilities (e.g. facial recognition, surveillance)

Limiting access to sensitive AI capabilities (e.g. facial recognition, surveillance)

GPSC keeps sensitive or high-risk AI capabilities such as facial recognition, biometric identification and surveillance-related systems, or any AI handling sensitive personal data, under tight control, so that only authorized staff can use them and only under defined conditions.

What we do

- We identify and classify sensitive or high-risk AI applications and set out which use cases are approved, restricted or prohibited across the company.
- Access is limited through the IT and cybersecurity controls already in place, role-based access control, user authorization, multi-factor authentication, access logging and periodic access reviews.
- Before any sensitive AI system goes live, it passes through existing governance, cybersecurity, privacy, legal and procurement reviews.
- A person always stays in charge: management retains the authority to review, approve, intervene, override or suspend an AI activity when needed.
- GPSC does not permit AI used for manipulative behavior, exploitation of vulnerabilities, social scoring or unauthorized biometric surveillance, in line with applicable law and responsible-AI principles.
- Usage, access rights, incidents and compliance are monitored and audited on a regular basis through our normal cybersecurity, audit and operational-risk routines.

Limiting access to sensitive AI capabilities (e.g. facial recognition, surveillance)



AI VALUE REALIZATION

โครงการนำ AI ไปใช้งานจริง
เพิ่ม productivity
และสร้างคุณค่าใหม่ให้หน่วยงาน

AI VALUE REALIZATION PROGRAM 2026

"ถ้าคุณคือคนที่ต้องการนำ AI มาใช้งาน องค์กรพร้อมสนับสนุนคุณแล้ววันนี้"

เปิดรับคำขอ AI License และลงทะเบียนเรียนได้แล้ววันนี้ >> ส่งรับคำขอ AI License คลิก <<

ติดตามข้อมูลโครงการ ผ่าน AIVA Community บน Viva Engage ตลอดโครงการ

AI ที่องค์กรเตรียมให้

Microsoft 365 Copilot Google Gemini Claude



Authorized Access to Enterprise AI Tools

GPSC manages access to AI technologies through its **AI Value Realization Program**, ensuring that employees access only **approved AI platforms and enterprise AI licenses** provided by the organization. Participation in the programme requires registration for authorized AI licenses and onboarding through designated communication channels, supporting controlled deployment and responsible use of AI technologies across the company.

The programme promotes the use of approved AI tools, including Microsoft 365 Copilot, Google Gemini, and Claude, under organizational oversight. By restricting access to authorized users and company-approved AI solutions, GPSC helps reduce the risk of unauthorized or inappropriate AI use while supporting secure, responsible, and ethical AI adoption in line with existing information security and governance practices.

2. Distinct labeling of AI-generated content and outcomes of AI-driven decisions

Distinct labeling of AI-generated content and outcomes of AI-driven decisions

GPSC is transparent about when AI is involved. Where AI materially contributes to content or influences a decision, we clearly identify or disclose that the content or outcome was generated or assisted by AI, enabling users to distinguish AI-generated information from human-created content and make informed decisions about how they use or rely on it. We also inform users when they are interacting with an AI system rather than a colleague.

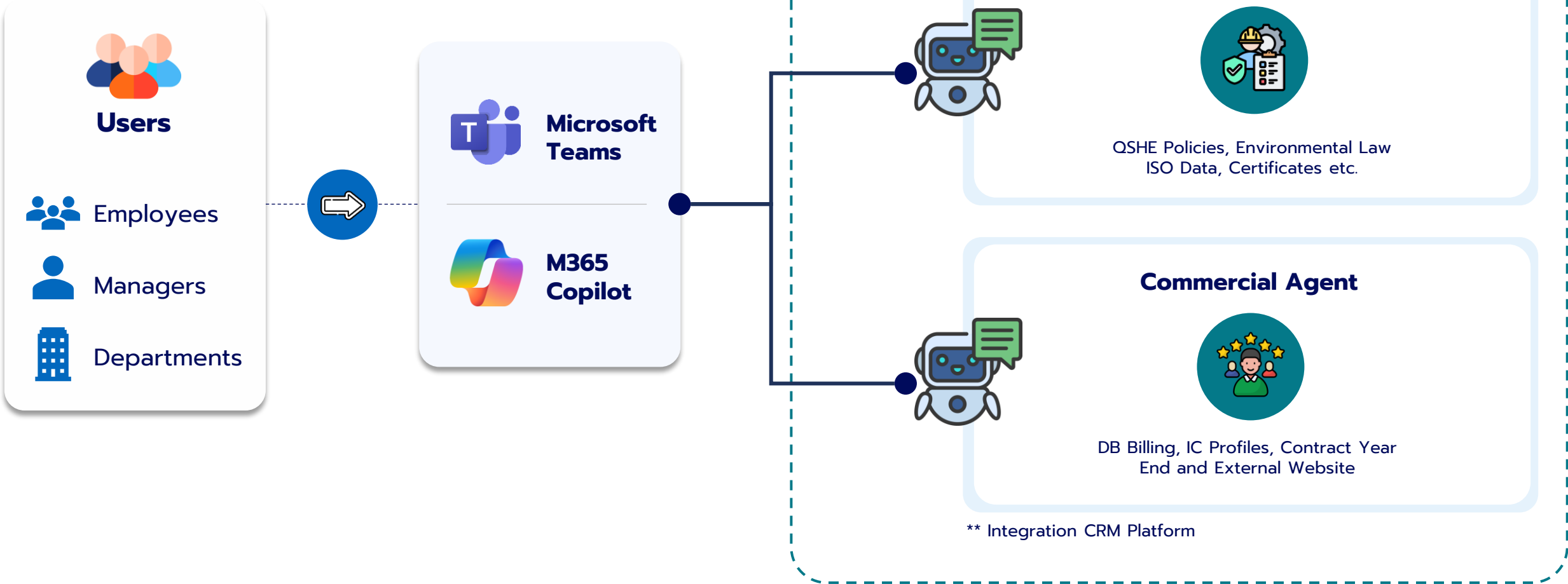
What we do

- Our guidelines call for AI-generated content and AI-driven decisions to be identified or disclosed where appropriate, and set out when labelling or notification is required for users, customers, employees or other stakeholders.
- AI output used in external communications, reporting, customer interactions or decision-making is checked and signed off by a responsible person before it is released.
- Users know when they are talking to AI. Where GPSC deploys chatbots or virtual assistants, such as the enterprise assistant “QSHE Agent and Commercial Agent”, used for QSHE and Commercial questions. people are told they are interacting with an AI system, and responses carry a reminder to verify information before relying on it.
- We keep documentation and traceability of AI-generated output and AI-assisted decisions so they can be explained and audited later.
- Labelling and disclosure practices are reviewed periodically against our internal governance, applicable regulations and responsible-AI principles.

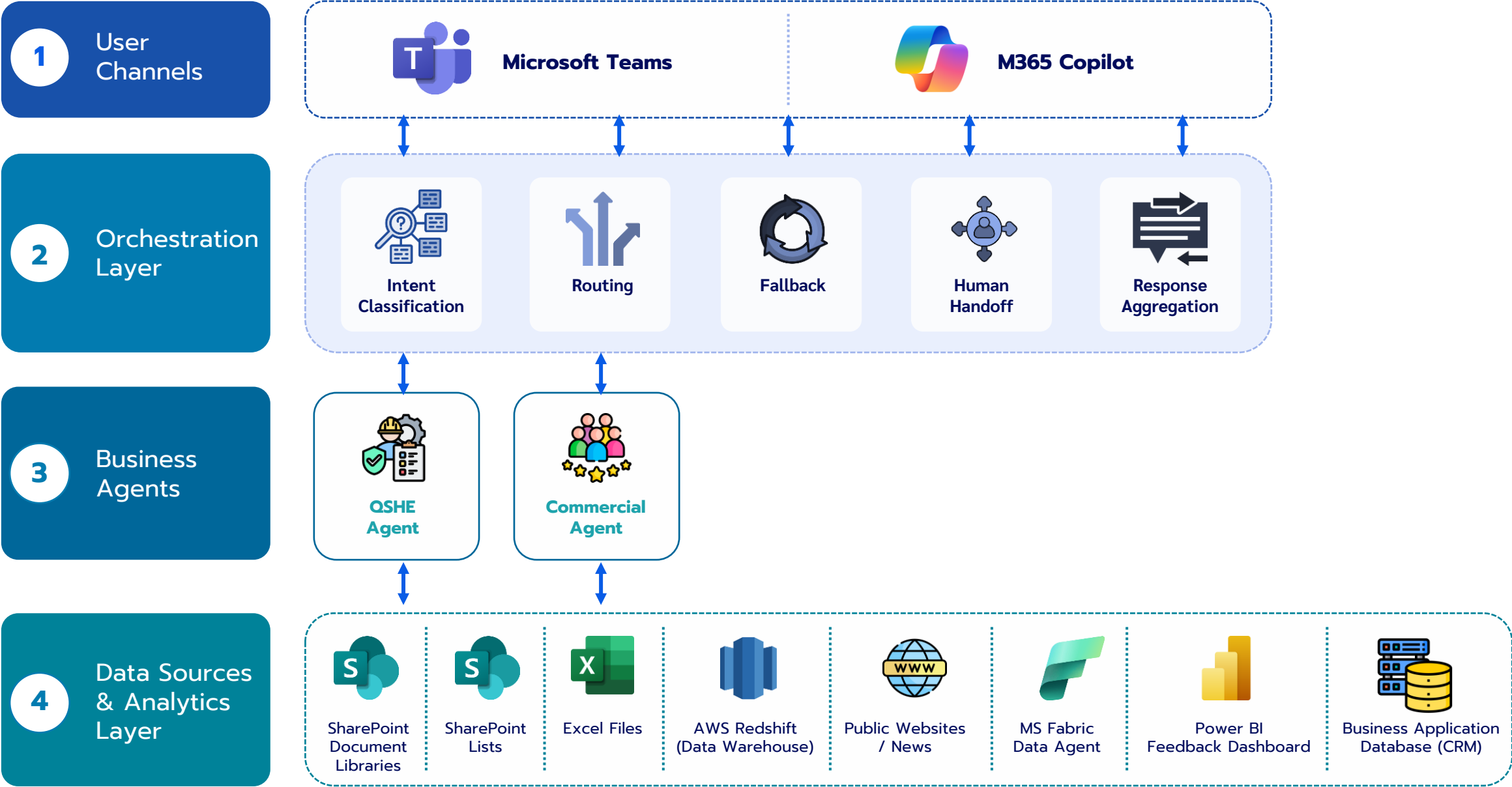
GPSC Corporate AI Agent



 Microsoft Teams + M365 Copilot Only



Solution Architecture



3. Mechanisms to detect and correct drift or degradation of AI models over time

Mechanisms to detect and correct drift or degradation of AI models over time

AI models can lose accuracy over time as data patterns or operating conditions change, what is known as model drift. GPSC watches its deployed models across their lifecycle and corrects them so they stay reliable and fit for purpose.

What we do

- We monitor model performance, accuracy, output consistency and data quality on an ongoing basis to spot drift or degradation early.
- Drift-detection and observability checks flag deviations in data patterns, operating conditions or model outputs, including concept drift.
- For critical use cases, a human validates the output and carries out periodic reviews to confirm it remains reliable and aligned with operational needs.
- When something looks wrong, we run a root-cause investigation and then apply corrective action, retraining, recalibration, adjusting parameters or thresholds, updating datasets, or rolling back and re-test before the model returns to production.
- (In practice) the “AI Bad Actor” predictive-maintenance system. The model learns from power-plant maintenance history and operating data, applies sensitivity and adversarial testing, and standardizes its output to the ISO 14224 failure-mode classification so results stay consistent and trustworthy as conditions change. It runs on Azure AI Foundry and is designed to be re-trained and re-deployed across plants.

AI BAD ACTOR PROVEN RESULTS

Predict. Prevent. Perform.
AI-Powered Reliability for a Sustainable Future



AI BAD ACTOR SOLUTION

Predictive Maintenance System

DATA SOURCES

- Equipment Sensors
- Historical & CMMS
- Logs & Events
- Operating Conditions



AZURE AI FOUNDRY AI/ML Models

1. Historical Learning LLM
2. Repair Notification Suggestion (Equipment Class, Failure Mode)
3. Close Work Order Suggestion (Failure Mechanism, Failure Cause)
4. Bad Actor Identification

INSIGHTS & ACTIONS

- Early Warning & Risk Score
- Failure Mode Classification (ISO 14224)
- Root Cause Analysis
- Maintenance Recommendation
- Dashboard
 - Risk Overview
 - Asset Health (High/Medium/Low)
 - Top Risk Assets (Asset, Risk Score, Failure Mode)



BUSINESS IMPACT

↓ **OPPORTUNITY LOSS**

↑ **INCREASE RELIABILITY**

STANDARDIZED & TRUSTED



Automatic Failure Mode Classification — Aligned with ISO 14224 for consistent and reliable insights

DATA INGESTION
(Collect & Integrate)



AI PROCESSING
(Train & Detect)



PREDICT
(Predict Failures)



RECOMMEND
(Recommend Actions)



ACT & IMPROVE
(Execute & Learn)

See the unseen. Prevent the unexpected.
Turning data into reliability and performance.



Equipment Reliability



Safety & Risk Reduction



Lower Downtime



Operational Excellence



Sustainable Value

Scalable. Repeatable. Real Results. — Ready to replicate across multiple power plants.

4. Regular assessments of deployed AI models for fairness/bias

Regular assessments of deployed AI models for fairness/bias

GPSC assesses its deployed AI models for fairness and bias on a regular basis, so that AI does not reinforce existing inequalities or create new forms of unfair treatment.

What we do

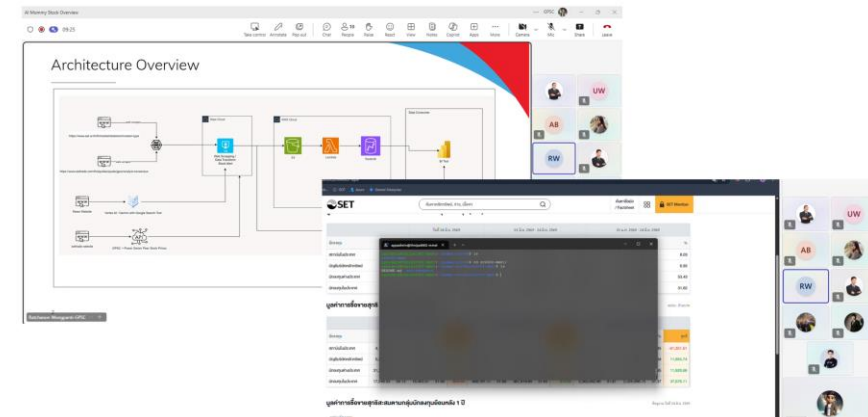
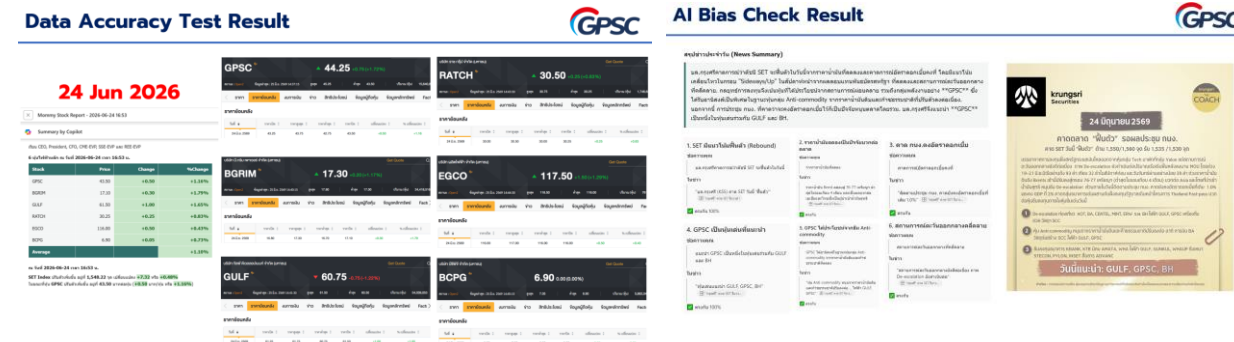
- Trained staff carry out regular, human-led fairness and bias reviews of deployed models and their output, identifying and mitigating fairness risks or unintended impacts across use cases.
- Reviews are kept relevant to the real operational and stakeholder context, and consider ethical risk, accountability and possible unintended effects.
- Cross-functional review and monitoring. involving the relevant stakeholders and control functions. drives continuous improvement and addresses emerging bias, transparency and ethical concerns across the AI lifecycle.
- How we test. We use AI fairness-checklist-style reviews with techniques such as slice-based evaluation (performance across groups), counterfactual and sensitivity testing (whether changing a protected attribute changes the outcome), and error-distribution analysis (whether errors fall fairly across groups).

Fairness starts with the data: GPSC manages training, validation and testing datasets for quality, diversity and representativeness, and controls data bias at source, in line with the AI Governance Guideline.

Regular assessments of deployed AI models for fairness/bias

AI Value Realization Program (AIVA) training sessions to equip employees with responsible AI practices, data governance, and secure AI adoption.

Human-led validation and bias assessment of AI model outputs before operational deployment.



5. Initiatives (own/with suppliers) to lower the ecological footprint of AI data centers/models

Initiatives (own/with suppliers) to lower the ecological footprint of AI data centers/models

As the flagship power and smart energy company of the PTT Group, GPSC pays attention to the energy and environmental footprint of the digital infrastructure behind AI, and favors energy-efficient and renewable-powered solutions.

What we do

- Our draft Responsible AI Policy commits to environmentally responsible AI energy-efficient systems, optimization techniques that reduce computational load, renewable-powered infrastructure, and attention to the energy, water and carbon intensity of AI operations.
- **We rely on enterprise cloud AI rather than heavy on-premise infrastructure.** GPSC uses managed enterprise services — Microsoft 365 Copilot (190 licenses), Google Gemini Enterprise (100 licenses) and Anthropic Claude (100 licenses) — which lets us draw on the efficiency and renewable-energy commitments of hyperscale providers instead of running energy-intensive AI hardware ourselves.
- Employee training encourages efficient use — writing better prompts and workflows to avoid unnecessary computation, checking output before re-running, and choosing a fit-for-purpose tool or model for the task.

It fits our clean-energy mission. GPSC's core business is producing and expanding clean energy, with an aspiration to be a top-three power company in Southeast Asia with more than half of its capacity from a green portfolio, on a pathway to Carbon Neutrality and Net Zero. That low-carbon power base supports the objective of a lower ecological footprint for AI.



AI ROADMAP to NET ZERO

Shaping a Sustainable Future with AI-Driven Clean Energy.



2026 : Adopt

Foundations & high-ROI quick wins

- Document Intelligence (OCR)
- Data Platform
- Generative AI (M365 Copilot, Gemini, Claude)
- Copilot Studio Adoption (AI Agents)
- Azure Foundry Platform



2027+ : Optimize

Scale analytics across assets

- Enterprise-Scale AI Deployment
- Digital Twin
- Plant Dispatch Optimization
- LLM Platform (Internal knowledge + operations)
- Advanced Forecasting (RE Platform)



OUR SUSTAINABILITY GOAL

NET ZERO EMISSIONS 2050

Every AI use case above also reduces emissions - fewer forced outages, higher plant efficiency, more renewables integrated into the grid, and smarter dispatch.

AI is not separate from the net-zero goal; it is one of the fastest levers toward it.

Systematically Manageable Challenges



Data Platform & Quality

Unified, governed operational and business data. Data prep drives up to 40% better model accuracy - start here, not with models.



AI Governance & Cybersecurity

Responsible-AI policy, model risk, data-leakage & prompt-injection controls, human-in-the-loop on safety-critical actions.



Talent & Change

AI literacy for all staff, deep skills for a central team, and process redesign — value comes from changing workflows, not bolting AI on.



EXPLAINABLE AI

Unlocking Understanding: Bridging the Gap to a Future of Visible Logic, Unwavering Trust, and Data-Informed Power.

6. Appeals process for users/affected third parties to contest an AI decision or outcome

Appeals process for users/affected third parties to contest an AI decision or outcome

People affected by an AI-driven decision can raise a concern or contest the outcome. GPSC does not build a separate silo for this. It routes AI-related concerns through the grievance, complaint and whistleblowing channels the company already has, with human review and clear resolution steps.

What we do

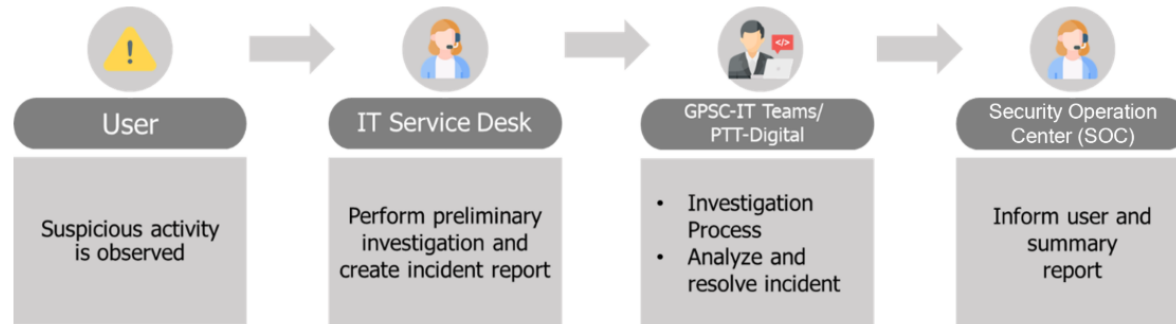
- AI-related appeals, complaints and incident reports are handled through existing ethics, grievance, compliance, whistleblowing, customer-service and operational-risk channels, so employees, customers, suppliers, contractors and other affected parties have a way to be heard.
- Clear escalation, review and resolution steps are defined. Who is responsible, response timelines, investigation steps and communication channels.
- A contested AI decision goes to appropriate human review, with the authority to validate, override, revise or escalate it (human-in-the-loop / human-over-the-loop).
- Records of appeals, investigations and corrective actions are kept to support accountability, transparency and continuous improvement.
- We review complaint and appeal trends periodically to spot recurring issues, improve the systems, and prevent the same problem happening again.

Built on existing channels. GPSC's established grievance and complaint-handling mechanisms, including its whistleblowing channel and the corporate complaint/dispute-resolution process under Risk & Crisis Management provide the foundation for contesting AI-related outcomes.

Appeals process for users/affected third parties to contest an AI decision or outcome

Integration of Appeals Process for Users to existing process

If any employee is found to have acted inappropriately or becomes a victim of the phishing test, GPSC will conduct targeted communication and organize training programs to raise awareness and enhance understanding of cyber threats among specific employee groups. In cases involving information security or cybersecurity incidents, employees are encouraged to contact the designated IT service channels, such as the IT Service Desk, system administrators, or PTT-Digital, to report the incident and initiate investigation and corrective actions.



Integration of Appeals Process for Affected Third Parties to Existing Process

Whistleblowing Process and Whistleblower Protection

GRI 2-24, 2-25, 2-26, 2-27

To ensure that the operation of GPSC as well as its subsidiaries and associates is efficient, compliant with laws, corporate governance policy, and the code of conduct, and is guided by transparency, fairness, and accountability, Whistleblowing and Complaints Handling Policy and announced the process for handling complaints and protect parties, along with mechanisms for monitoring and investigating complaints in order to prevent risks and protect and protect whistleblowers submitting reports in good faith

(Link)

Whistleblowing training



From 1 January 2024 to 31 December 2024, the company no complaint regarding corruption.

WHISTLEBLOWING CHANNELS

- **Mailing Address:** Addressed to Corporate Governance and Compliance Department or Human Resources and Organization Development Department
Address: Global Power Synergy Public Company Limited
555/2 Energy Complex, Building B, 5th Floor Vibhavadi Rangsit Road, Chatuchak Sub-district, Chatuchak District, Bangkok 10900
- **E-mail Address:**
whistleblowing_complaint@gpscgroup.com
- **E-Website:**
<http://www.gpscgroup.com/th/cg/whistle-blowing>
<http://www.gpscgroup.com/en/cg/whistle-blowing>
- **In person:** Submit the report to Corporate Governance and Compliance Department or Human Resources and Organization Development Department.
- **Report to the Board of Directors or Management** through any available channel such as a letter, e-mail, or in person. The Board of Directors or Management shall then forward the matter to Corporate Governance and Compliance Department and/or Human Resources and Organization Development Department in order to proceed in accordance with "Section 2: Complaint Handling Process."

Appeals Process for Users and Affected Third Parties

- GPSC integrates AI-related concerns, complaints, and requests for clarification into its existing incident management and whistleblowing processes, providing users and affected third parties with accessible channels to raise concerns regarding the use or outcomes of AI technologies. Rather than establishing a standalone AI appeals mechanism, AI-related cases are managed through established governance processes that support transparency, accountability, and appropriate oversight.
- For internal users, AI-related concerns or suspected inappropriate AI outcomes can be reported through the **IT Service Desk**, where incidents are logged, subject to preliminary assessment, and escalated to the relevant GPSC IT teams or PTT Digital for investigation and resolution. Where cybersecurity or information security implications are identified, cases are further escalated to the **Security Operation Center (SOC)** for detailed investigation, corrective actions, and communication of investigation outcomes.
- For external stakeholders and affected third parties, GPSC provides established **whistleblowing and complaint channels** through which concerns related to AI use, ethical conduct, or potential adverse impacts may be submitted. Reported cases are reviewed, investigated, and handled in accordance with the Company's governance, complaint-handling, and whistleblower protection procedures to ensure that concerns are addressed fairly, consistently, and under appropriate organizational oversight.
- By leveraging these existing governance mechanisms, GPSC provides clear pathways for users and affected third parties to report AI-related concerns, seek clarification regarding AI-assisted outcomes, and request that reported issues be investigated through established organizational processes, thereby supporting accountability, transparency, and responsible AI governance.

1. Ref: [Risk & Crisis Management | Global Power Synergy Public Company Limited \(GPSC\)](#)
2. Ref: [20220606-gpsc-cdcr-manual-en \(v.2\)](#)

7. Quantification of the impact of AI initiatives/tools on sustainability outcomes

Quantification of the impact of AI initiatives/tools on sustainability outcomes

GPSC measures how its AI work contributes to sustainability, energy efficiency, emissions, resource use, reliability and productivity and uses those metrics to make accountable, data-driven decisions.

What we do

- We track the environmental, operational and social impact of AI-enabled initiatives, including contributions to energy efficiency, emissions reduction, resource optimization, reliability and workforce productivity.
- Relevant metrics and KPIs are developed to quantify outcomes for example, reductions in downtime, maintenance cost, energy use, emissions or process inefficiency and folded into existing ESG, digital-transformation and sustainability-reporting processes.
- Every use case is tied to tracked value. Under GPSC's AI roadmap, each AI use case is linked to a measured benefit in Baht, MW or CO₂, with engineering sign-off, so its contribution is quantified and each phase helps fund the next.
- A concrete result AI Bad Actor. The "AI Bad Actor" predictive-maintenance programmed is reported to have reduced opportunity loss. By catching equipment problems earlier and reducing unplanned downtime, it supports higher plant efficiency and, in turn, lower emissions.

AI and analytics also support sustainability-related forecasting, optimization, predictive maintenance and smart energy management, and AI-enabled projects are reviewed periodically for effectiveness, business value and sustainability contribution.

Quantification of the impact of AI initiatives/tools on sustainability outcomes



GPSC applies responsible and resource-efficient AI adoption practices to limit the computational and energy footprint of its AI usage. This includes selecting fit-for-purpose AI tools and models for each use case, and monitoring the utilization and value of enterprise AI licenses so that under-utilized licenses can be reassigned or retired rather than left idle reducing unnecessary computational load and resource consumption associated with AI operations. Employee guidance on efficient AI use (e.g., optimizing prompts and workflows and validating outputs to avoid repeated processing) further supports this objective. The license-utilization review process is currently being implemented, with results being compiled to inform ongoing optimization.

More than 90% of employees eligible to use the licenses had their access renewed based on demonstrated results showing improvements in work efficiency, including time savings, workforce optimization, and reduced operating costs.

8. Training of employees on the ethical use and/or security of AI

Training of employees on the ethical use and/or security of AI

GPSC is building an AI-literate, responsible workforce. Employees are trained to use AI ethically and securely, so they make informed decisions and uphold the company's responsible-AI standards.

What we do

- Training and awareness programmes cover the responsible, ethical and secure use of AI, data privacy, cybersecurity, bias awareness, human oversight and responsible decision-making.
- AI Value Realization Program ("AIVA"). A structured employee journey from license approval and activation through to AI learning sessions, that deliberately manages skills gaps, trust and data governance while helping people use enterprise AI tools such as Microsoft 365 Copilot and Copilot Studio responsibly.
- AI Bootcamp and executive enablement. Hands-on training across four sessions on M365 Copilot and AI agents (Power Automate, Copilot Studio) turns real business cases into working use cases, complemented by an executive discovery workshop and the "Make IT Happiness" security-awareness activity.
- Clear Gen AI Do's and Don'ts. The Generative AI Policy tells employees not to put confidential or personal data into public AI tools, not to register for public AI with a corporate email, to verify AI output before use, and to keep a human in the loop for decisions reinforcing both ethics and security.

Role-based upskilling and periodic refresher sessions keep the workforce current on evolving AI regulation, cybersecurity threats and responsible-AI practice, and responsible-AI principles are embedded in internal guidelines.

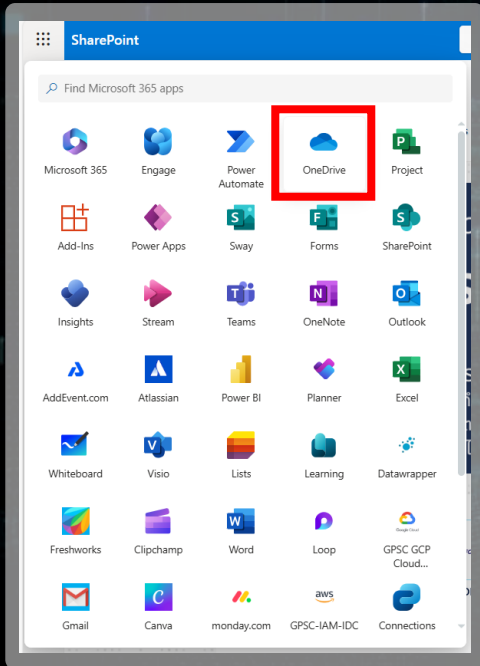
Stop Oversharing: Secure Your OneDrive Files Today!



Learn how to review and stop sharing files or folders that no longer need external access.

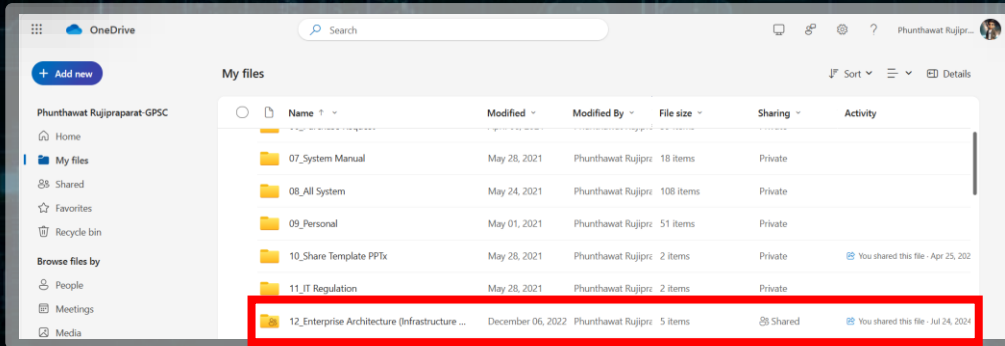
1

Open OneDrive in your browser or via the desktop app.



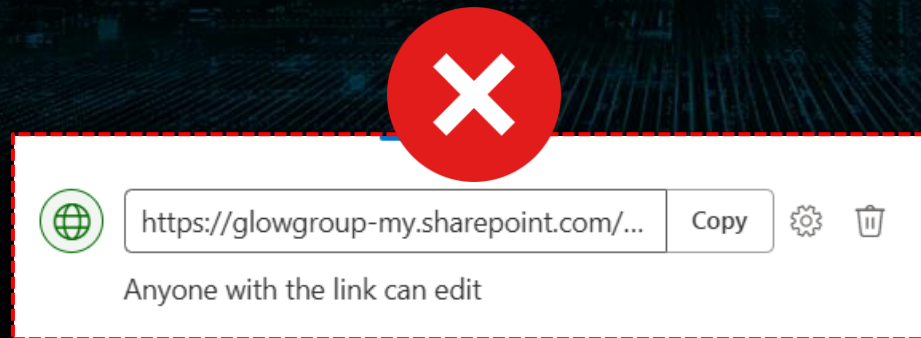
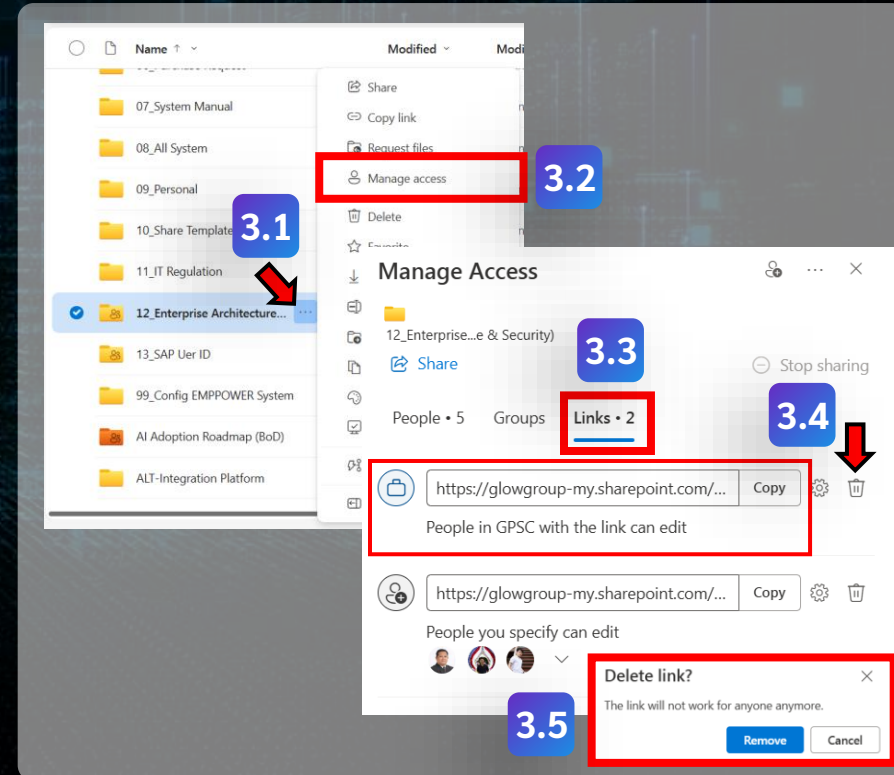
2

Navigate to the file or folder you want to stop sharing.



3

Right-click the item and select "Manage access" and Click "Remove Link"



Sharing files on OneDrive is **convenient** - but oversharing can lead to unintended **data exposure**.



People First. Future Forward

Empowering People, Transforming Culture



GPSC GROUP IT DAY
Security Awareness "Make IT Happiness"



**GPSC DATA REVOLUTION
BOOTCAMP**

GPSC | Employee Collaboration Activity

AI Bootcamp



The working committee organized an AI training course for employees to develop use cases. The course focused on building an understanding of the technology to efficiently apply it to future applications, such as using Power Automate and Copilot Studio. **4 Sessions (M365 Copilot & Agents)**



AI Value Realization Program (AIVA)



AI TOOLS



M365 Copilot



Copilot Studio

PEOPLE AT THE CENTER.
AI AS OUR ASSISTANT.
VALUE TOGETHER.



WHAT WE
MANAGE
CAREFULLY



SKILLS GAP



TRUST



DATA
GOVERNANCE



AI VALUE REALIZATION PROGRAM 2026

โครงการนำ AI ไปใช้งานจริง เพิ่ม productivity และสร้างคุณค่าใหม่ให้หน่วยงาน

"ถ้าคุณคือคนที่ต้องการนำ AI มาใช้งาน องค์กรพร้อมสนับสนุนคุณแล้ววันนี้"

เปิดรับคำขอ AI License และลงทะเบียนเรียนได้แล้ววันนี้

>> ส่งรับคำขอ AI License คลิก <<

ติดตามข้อมูลโครงการ ผ่าน AIVA Community บน Viva Engage ตลอดโครงการ

AI ที่องค์กรเตรียมให้



Microsoft 365 Copilot



Google Gemini



Claude

Limiting access to sensitive AI capabilities (e.g. facial recognition, surveillance)

GPSC **ระวัง! AI ถูกใช้เป็นอาวุธโจมตีคุณ**

ความรุนแรงของภัยคุกคาม AI ในปี 2026

- 4.5 เท่า** ประสิทธิภาพสูงกว่าเดิม
AI Phishing มีอัตราความสำเร็จสูงถึง 54% เมื่อเทียบกับแบบเดิมที่เพียง 12%
- 87%** ขององค์กรที่โดนโจมตีโดย AI
- ภัยคุกคามอันดับ 1** การโจมตีที่ขับเคลื่อนด้วย AI กลายเป็นภัยคุกคามอันดับ 1 ที่ทุกองค์กรต้องเผชิญ

ภัยคุกคาม AI

- AI Spear Phishing**: วิศวกรที่พบบ่อยเพื่อปลอมแปลงอีเมลบุคคลที่มีตัวตนจริง
- Voice & Video Deepfake**: ปลอมแปลงใบหน้าและเสียงของผู้บริหารเพื่อใช้ในการหลอกลวง
- Malware**: โปรแกรมประสงค์ร้ายที่เข้ามาฝังในข้อมูลหรือทำลายระบบ
- AI BEC**: เชื่อมแบบอัตโนมัติการแจ้งเตือนจากผู้บริหารได้อย่างแม่นยำ

มาตรการ "หยุด - ยืนยัน - แจ้ง"

1. หยุด เมื่อสงสัย
2. โทรยืนยันโดยตรง
3. แจ้ง IT Servicedesk ทันที

5 สัญญาณเตือนภัย (Warning Signs)

- กดปุ่มเร่งด่วน (Urgency Pressure)
- Domain/URL ปลอม (Fake Domain/URL)
- วิดีโอกระตุก (Video Glitches/Artifacts)
- ขอ OTP โดยไม่คาดคิด (Unexpected OTP Request)
- ภาษาแปลกๆ (Unusual Language/Phrasing)

รายการเร่ง - ป้องกันได้: การแจ้งเหตุกับทีมช่วยยืนยันข้อความเสียหายน่าจะหายไป

Contact: servicedesk@pttdigital.com | GPSC Cybersecurity Awareness

GPSC **ใช้ AI อย่างไรให้ปลอดภัย: คู่มือพนักงานและบทลงโทษที่ควรรู้**

ข้อปฏิบัติและข้อห้ามสำคัญ (Do & Don't)

- ตรวจสอบความถูกต้องและอ้างอิงแหล่งที่มาทุกครั้ง**
AI เป็นเพียงผู้ช่วย พนักงานต้องเป็นผู้ตัดสินใจ และตรวจสอบผลลัพธ์ก่อนนำไปใช้งานจริงเสมอ
- ห้ามป้อนข้อมูลความลับหรือข้อมูลส่วนบุคคลลงใน AI สาธารณะ**
เพื่อป้องกันความเสียหายข้อมูลรั่วไหลสู่ภายนอกที่บริษัทไม่สามารถควบคุมได้
- ห้ามใช้อีเมลบริษัทสมัครใช้งาน AI ภายนอก**
ต้องได้รับอนุมัติก่อน และควรตั้งค่าความเป็นส่วนตัวส่วนตัวให้ปลอดภัยเสมอ

คำเตือนและบทลงโทษ (Warning & Penalties)

- AI คือเครื่องมือช่วยงาน ไม่ใช่ผู้ตัดสินใจแทน**
พนักงานต้องรับผิดชอบต่อผลลัพธ์ของงานที่ได้จาก AI 100%
- Personal Gen AI ไม่ได้อยู่ภายใต้การควบคุมของบริษัท**
ข้อมูลที่ป้อนอาจถูกจัดเก็บภายนอก ซึ่งเสี่ยงต่อการรั่วไหลของข้อมูลองค์กร
- หากตรวจพบการนำความลับหรือข้อมูลธุรกิจของบริษัทไปใส่ใน AI สาธารณะ: ระดับความผิด: เล็กจางโดยไม่จ่ายค่าชดเชย**

ระวังภัย! AI สรุปรงานฟรี... หรือกับดักลวงความลับ?

รูปแบบกลโกงและจุดสังเกต (The Trap & Red Flags)

รูปแบบกลโกงสุดเนียน

ส่อลวงด้วยการสรุปเอกสารฟรีเพื่อแลกเก็บข้อมูลความลับขององค์กรหรือข้อมูลส่วนตัว

สัญญาณอันตราย (Red Flags)

- ขอสิทธิ์เข้าถึงข้อมูลที่ไม่จำเป็น
- แหล่งที่มาที่น่าเชื่อถือ

แนวทางปฏิบัติเพื่อความปลอดภัย (Call to Action)

สิ่งที่ต้องทำเมื่อเจอภัย

- หยุดการให้ข้อมูลทันที
- ตรวจสอบความน่าเชื่อถือของเว็บไซต์
- และแจ้งเตือนผู้อื่น

ป้องกันข้อมูลรั่วไหล

หลีกเลี่ยงการใส่ข้อมูลสำคัญหรือความลับบริษัทลงในเครื่องมือ AI ที่ไม่ผ่านการรับรอง

Employee Training on the Ethical and Secure Use of AI

GPSC promotes the responsible, ethical, and secure use of AI through organization-wide awareness campaigns and employee guidance on AI-related cybersecurity risks and good practices. Employees receive practical guidance on the safe use of AI tools, including verifying AI-generated information before use, protecting confidential and personal information, recognizing AI-enabled cyber threats such as phishing, deepfakes, and business email compromise (BEC), and reporting suspicious activities through established cybersecurity channels.

The awareness programme reinforces that AI is a tool to support, rather than replace, human judgment and accountability. Employees are prohibited from entering confidential or business-sensitive information into public generative AI platforms and are reminded to use only authorized AI solutions in accordance with the company's information security requirements. These initiatives help strengthen employees' awareness of AI security risks, promote responsible AI use, and reduce the risk of data leakage, cyber threats, and inappropriate use of AI technologies across the organization.

9. The AI management system verified

The AI management system verified (e.g. ISO42001)

GPSC is strengthening its AI management system and positioning it for independent, third-party verification against recognized standards such as ISO/IEC 42001. We are candid that this is a direction of travel: the management system is being aligned with the standard, and formal external certification is a forward-looking commitment rather than something already achieved.

Where we are, and where we are heading

- A standards-aligned foundation. GPSC's AI Governance Guideline and draft Responsible AI Policy are written with reference to internationally recognized standards ISO/IEC 42001:2023 (AI Management System), the NIST AI Risk Management Framework, ISO/IEC 23894 (AI risk management) and ETDA's Generative AI guidance which gives us a management-system basis suited to future external verification.
- What ISO 42001 covers. Published in 2023, ISO/IEC 42001 sets requirements for an AI Management System (AIMS) covering the full AI lifecycle, addressing algorithmic bias, transparency, model drift, data quality and accountability. GPSC intends to align its management system with these requirements.
- Our roadmap envisions pairing an ISO 42001-aligned AIMS with complementary standards already familiar to the organization, such as ISO/IEC 27001 for information security, to form a single governance framework across AI, data, privacy and operational resilience.
- As part of continuous improvement, GPSC plans internal reviews and readiness assessments of the AI management system, with the aim of pursuing third-party verification as the Responsible AI Program matures in line with the CSA "best practice" of externally verifying the AI management system.

THANK YOU

