Artificial Intelligence Security Policy

Artificial Intelligence (AI) introduces new opportunities for innovation, but it also presents new risks that must be managed to safeguard our people, data, services and clients. At Capita, we are committed to ensuring that all AI systems, tools, and processes are designed, deployed, and operated securely to protect against malicious use, unauthorised access, and operational disruption.

The policy outlines our commitments and expectations regarding the security of AI technologies across Capita.

We are committed to:

- Embedding security by design into AI initiatives, ensuring systems are robust, resilient, and aligned to Capita's Information Security policies.
- Protecting AI models, data, and outputs against tampering, leakage, or manipulation.
- Managing supply chain and third-party AI risks to ensure all external providers meet Capita's security requirements.
- Implementing continuous monitoring and improvement to adapt to emerging AI security threats and vulnerabilities.
- Ensuring secure integration of AI systems with existing IT and business processes, minimising unintended security risks.
- Maintaining clear accountability and oversight for AI-related security incidents and vulnerabilities.
- Adhering to our legal, regulatory, and industry-specific obligations relating to AI.

Artificial Intelligence activities must align with:

- Capita Information and Cyber Security Policy.
- Capita Code of Conduct.
- Capita's values and Responsible AI Principles.
- Capita's Data Ethics Standard.
- Secure development and coding standards.
- Legal and regulatory requirements, including local, national, and international laws.
- Contractual obligations.
- Related policies and standards:
  - Data Privacy
  - Data Governance
  - Incident Management
  - Supply Chain and Vendor Risk Management
  - Business Continuity and Disaster Recovery

What you should expect from us:

Monitor and manage security vulnerabilities and risks associated with AI across Capita. In addition, we maintain various standards, which:

- Ensure transparent AI use, with clear communication when AI is used in products, services, or decisions that affect Capita employees or users.
- Ensure AI models, databases, and outputs are protected from unauthorised access, theft, or misuse.
- Provide security standards and controls for the secure deployment and operations of AI systems.
- Provide training and awareness resources on secure AI use, including how to detect and report suspicious AI activity.
- Maintain incident response processes tailored to AI-specific threats from malicious use or compromise.
- Define accountability frameworks, roles and escalation paths for AI-related security incidents.

What we expect from you:

- Only use AI systems securely and in line with this policy and Capita’s Information Security standards.
- Keep up to date with Capita AI guidelines, training, and updates as they evolve.
- Protect AI systems and outputs from unauthorised disclosure or sharing.
- Do not attempt to bypass security controls, safeguards, or monitoring mechanisms in AI tools.
- Ensure AI-related code, prompts, and outputs are classified, labelled, and handled securely.
- All data used for AI interaction must be handled in accordance with relevant data protection laws, regulations and Capita’s Data Governance Standard.
- Adopt a transparent approach to the use of AI.
- Abide by any relevant licensing conditions regarding intellectual property rights in the authorised AI platform's terms of use.
- Challenge any requested use that contradicts this policy or introduces a security risk.
- Report security concerns or anomalies in AI systems promptly via the Incident Reporting Process.

How will we achieve this:

- Collaborate with the Capita AI, Cloud and Data Compliance and Monitoring Committee (**AICAM**) to embed robust security practices into AI governance, ensuring technology oversight includes protective risk management, secure design principles and continuous assurance.
- Embed AI security principles into Capita’s governance, risk, and compliance frameworks.
- Adopt hyperscaler well-architected frameworks to ensure consistent delivery of robust security practices.
- Regularly review AI security controls through risk-based monitoring, assurance reviews, and internal audits.
- Apply threat modelling to AI systems to identify and mitigate vulnerabilities.
- Ensure cross-functional engagement with Information and Cyber Security, Risk, Legal, HR, and business units in AI design and deployment.
- Track key performance indicators relating to AI security effectiveness.
- Ensure all security incidents are reported and managed through established governance mechanisms, up to Group Risk Committees where required.

Manpreet Singh
CTO, Capita plc
December 2025