Capita

Cyber Psychological Safety Policy

Capita is dedicated to maintaining a working environment where psychological safety is paramount. By ensuring that internal cybersecurity assessments are used as tools for positive change rather than punishment, we can build a more secure and supportive workplace for everyone. This policy establishes a framework to ensure that all cybersecurity assessments are conducted to promote positive improvement and learning where colleagues feel confident that assessments will not be used as a tool for punishment but rather as an opportunity for growth and development. Furthermore, this policy protects individuals who raise concerns about potential risks, ensuring they are supported and safeguarded from any form of retribution, thereby fostering a culture of openness and accountability.

We are committed to:

- Fostering a culture of psychological safety within our cybersecurity practices, ensuring that all colleagues can engage without fear of blame or retribution.
- Using internal assessments, such as phishing exercises, penetration tests, and incident reviews, as tools for improvement and learning rather than for punishment or disciplinary action.
- Maintaining a non-punitive environment where the focus is on collective growth and development, ensuring that errors and vulnerabilities lead to stronger security measures.
- Encouraging open communication and collaboration, so all team members can contribute to strengthening Capita's cybersecurity defences without fear of negative consequences.

In line with our:

- Information & Cyber Security Strategy & Policy.

What you should expect from us:

- Safe environment where all contributions to cybersecurity practices are valued, and there is no fear of blame or reprisal.
- Transparency in internal assessments which will be used solely to identify areas for improvement.
- Fair and non-punitive responses to any security vulnerabilities or incidents, with the aim of fostering learning and enhancing our collective knowledge.

What we expect from you:

- Engage openly and honestly in all cybersecurity assessments, sharing relevant information to help identify areas for improvement.
- Embrace a culture of learning and growth, recognising that assessments are designed to strengthen our security, not assign blame
- Actively contribute with constructive feedback and collaboration.
- Follow cybersecurity protocols and best practices, supporting Capita's ongoing efforts to enhance security.
- Reach out to your line manager for help and guidance when you don't understand something.
- Remain proactive and vigilant, reporting any security concerns or vulnerabilities promptly to help protect Capita.

What we expect from our managers:

- Lead by example, encouraging open communication and treating cybersecurity assessments as opportunities for learning and improvement.
- Provide constructive feedback and support their teams in addressing vulnerabilities and implementing necessary improvement.
- Ensure that internal assessments are conducted fairly and transparently, with a clear focus on strengthening Capita's security, not assigning fault.
- Recognise and promote a growth mindset, helping their teams view assessments as chances for development and reinforcing the importance of collaboration and continuous improvement.

How we will achieve this:

- Ensure transparency in our assessment processes, with clear communication on how findings will be used to drive improvements and avoid creating a punitive atmosphere.
- Foster continuous collaboration and feedback by engaging teams in discussions on assessment outcomes, encouraging shared responsibility for security improvements across Capita.
- Provide regular training and support to ensure all colleagues and managers understand the purpose of assessments and how they contribute to a safer and more secure working environment.

Manpreet Singh

Chief Technology Officer

October 2024