Guidance on Fraud Prevention July 2025

The infiltration of organizations by fraudulent individuals posing as legitimate employees or contractors is a growing and sophisticated threat affecting the global IT services ecosystem. Such actors often use forged identities, deep-fake technologies, and masked locations to bypass standard hiring checks and gain access to sensitive systems and data.

In the interest of data and information security, Bayer expects its suppliers to take actions in preventing the risk of infiltration with fraudulent individuals as employees or contractors. Please refer to the following guidance:

- **Conduct robust identity verification** for all new hires, including contractors and remote workers. This may include in-person validation, background checks, and the use of third-party verification tools. This should also include periodic background checks proportional to the role's risk level, covering global and country-specific databases.
- **Monitor for anomalies** in access patterns or remote desktop tooling, especially from remote or offshore personnel.
- **Train your hiring and HR teams** to recognize red flags such as inconsistent documentation or evasive behavior.
- **Report any suspected fraudulent hires** to Bayer immediately.

Should you discover that a fraudulent individual has been hired and granted access to Bayer systems or data, we expect:

- Immediate revocation of access.
- **Prompt notification to Bayer via email to Bayer's CSOC (Cyber.Security.Operation.Center@Bayer.com).**
- Full cooperation with our investigation and remediation efforts.

We understand the challenges of managing a secure and scalable workforce, and we are committed to working with you to uphold the highest standards of trust and integrity across our shared digital ecosystem.

Thank you for your continued partnership and vigilance.