Case study two: Student visitors

Following an agreement between their two institutions, a cohort of overseas Master's students spent six months at a UK university. The students were expected to attend classes on campus and were assigned academic supervisors.

Although financial checks were completed before the agreement was finalised, further due diligence was not. Specific checks were not conducted to ensure compliance with UK strategic export controls.

Supervisors had minimal interactions with the students, assuming the visit co-ordinator to be in regular contact with them. This left the students unsupervised and free to approach researchers and ask to collaborate with them, as is normal academic practice.

Following multiple approaches, several students became involved in highly sensitive, export-controlled research projects and gained access to restricted facilities.

A request for access to a computing facility was granted by the co-ordinator with no additional oversight. The students shared the single-access card to visit the lab and other controlled areas.

Learning points

The university should have conducted a review of the work being undertaken. If the technology was controlled, an export licence should have been requested.

A range of techniques can be used to identify and exploit vulnerabilities at UK higher education institutions.

Locations containing sensitive research and materials must be appropriately protected. Following this breach, the card-operated door was replaced with turnstiles, to prevent multiple entries with a single card.

Clear management and oversight processes are required for visiting students and staff, including pre-arrival checks and regular points of contact. Supervisors of visiting staff must be aware of their obligations and responsibilities for the entirety of the visit.

Staff working on export control or dual-use technologies must understand and fulfil their obligations to protect their research and university IP, both at home and abroad.