"Cyber Essentials is the start of a continuing cyber security journey"

The University of Bath has almost 19,000 students, with 30% of these coming from overseas. Research is an important focus for each of its four faculties – engineering and design, humanities and social sciences, management and science. Employability is another focus and, in pursuit of these two goals, the university has developed its own Innovation Centre, fostering start-ups by providing a workspace, specialist expertise and business know-how to businesses that have developed from research or from students' own learning.

Protecting research integrity

In October 2020 the University of Bath applied for its Cyber Essentials (ncsc.gov.uk/cyberessentials/overview) certificate – wanting to audit its online security protections for compliance with funder requirements and also to safeguard its research interests.

"Bath is a research-intensive university working in sensitive areas such as energy generation and healthcare." **Dave Thatcher, security analyst at the university**

"Cyber Essentials is a government-backed scheme that may help organisations guard against problems like hacking, phishing and password guessing. We work with UK government departments that may require their research partners to have the Cyber Essentials certificate."

So do many other research funders as well as various organisations as part of their supply chain assurance.

At Jisc, we're an accredited Cyber Essentials certifying body meaning we can issue these certificates on behalf of IASME (iasme.co.uk/) and the National Cyber Security Centre (NCSC) (ncsc.gov.uk/). We can also help our members work through the certification process. Our Cyber Essentials service (jisc.ac.uk/cyber-essentials) includes Cyber Essentials drop-in clinics (jisc.ac.uk/training/cyber-essentials-drop-in-clinic) where people can ask specific questions, and tailored advice and guidance to help organisations get ready for the assessment. Members can use as much or as little support as they need.

"The best piece of advice I can give to institutions is to prepare thoroughly," says Dave. *"We wanted to gain the certificate quickly and cost effectively and Jisc's help made that possible. We took time to prepare our answers and get the necessary information together, asking Jisc questions when we needed more information about what was required.*

"We always got an answer very quickly, along with advice and the names of technical specialists to speak to on specific points. We got through the assessment without a hitch and this was down to careful planning."

Cyber Essentials Plus

While Cyber Essentials is self-assessed, the more advanced **Cyber Essentials Plus** (jisc.ac.uk/cyber-essentials) involves internal and external testing. This more detailed process verifies the information provided for Cyber Essentials and includes a series of tests to check a variety of end user devices. It's something that organisations can't do on their own so they'll need to come to an accredited certification body with trained and certified staff.

Taking this next step must be done within 90 days of achieving Cyber Essentials. The scope of work should be the same: a different scope would mean repeating Cyber Essentials, costing more money and taking longer.

> *"Here at Bath the scope for both focused on research infrastructure and systems – specifically our Windows 10 research desktops. As before, planning and some timely advice were key to a smooth process,"* says Dave.

"On testing day we had a kick-off call with Sam Eaton-Rosen [Jisc's senior **penetration testing** (jisc.ac.uk/penetration-testing) specialist], and then he was able to complete the tests and checks in an hour or so. It feels strange to put your systems through that but it was painless. Sam told us it was the quickest and smoothest testing he'd ever done.

> *"It was a no-brainer for us to get Jisc's support with Cyber Essentials and Cyber Essentials Plus. Its detailed knowledge of HE and FE makes Jisc the ideal partner."*

Was there anything that could have helped the university prepare any better?

> *"It was all new to us and, with hindsight, it would have been useful if the approval process was clearer from the start,"* says Dave. *"But Jisc were so responsive when we asked questions that this hardly mattered. And we'll understand it more when we do the re-certification next year.*
>
> *"We will get Jisc to help us then, too, because things can change and it's worthwhile to have that support."*

What's next?

> *"Next year we might extend the scope and, in the meantime, we are going for BS3 1111:2018,"* says Dave *referring to another of the cyber security assessment services run by JISC.*

BS 31111 (jisc.ac.uk/bs31111-audit-and-assessment) helps organisations of any kind and size identify cyber security risks and mitigate them appropriately. It is designed to promote a top-down approach to cyber resilience and improve operational performance.

> *"The HE sector is going down this path now. Cyber security risks are not an IT issue they're a whole organisation issue and we're working on keeping our security levels high in expectation of new and more complex threats."*

To find out how Jisc can support your organisation, please:

Contact:
securityservices@jisc.ac.uk

or visit
jisc.ac.uk/cyber-essentials