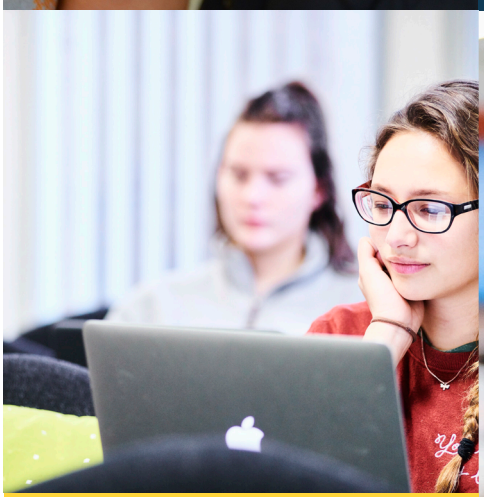
Durham University

Inspiring the extraordinary

Information and Cyber Security Strategy

December 2021



Introducing our information and security strategy

The University's Digital Strategy sets out the ways in which the organisation will make ever increasing use of digital technology to deliver benefits across its six strategic pillars:

- People
- Research & Engagement
- Education
- Accommodation, Estates & Infrastructure
- Wider Student Experience
- Global

People and information are two of the University's most important assets and both stand to benefit significantly from technological improvements. However, both are also subject to significant risk from abuses or failures of digital technology and the processes that surround it.

This Information and Cyber Security Strategy outlines how the University will develop and mature its organisational and technical controls alongside its use of digital technologies, to protect the interests of the organisation and the individuals that interact with it. At the same time, it must do this without undermining the flexibility and innovation needed to deliver world-class teaching and research.

The Strategy is for the whole organisation and is not just about implementing technical controls within CIS. Effective information and cyber security rely on every member of the organisation doing their part to protect the University's critical assets, themselves, and each other. Threats in the information and cyber security space evolve rapidly and this Strategy will similarly need to evolve. It will therefore be updated at least annually to ensure it continues to address the risks that are most relevant to the University.

Strategy vision

"Durham University is regarded as a trusted custodian of data by staff, students, partners and the public. This is achieved through the use of appropriate security controls to protect data and operations from the consequences of cyber attacks and information breaches, whilst minimising constraints on the individual ways of working that enable world-class teaching and research."

Why do we need a strategy?

Cyber and information security breaches have unfortunately become the new norm, with the average cost of a breach to an organisation estimated at £3.5m in the UK, while the average time for an organisation to identify and contain a breach is 287 days. Although large data protection fines grab the headlines, operational disruption can be at least as damaging. The harm and distress caused to individuals can also be considerable. Cyber attacks and information security breaches have now become important board-level issues, with many organisations highlighting them as significant risks (Figure 1).

Figure 1: Why do we need a strategy?

How will we improve information and cyber security?

Modern approaches to information and cyber security place an emphasis not only on defence, but on an organisation's ability to respond to and recover from a cyber incident. This is often referred to as cyber resilience and it includes the ability to **detect** an actual or potential compromise, **respond** to a security event, and **recover** from a compromise. Having controls in place to **protect** the environment is essential, but experience shows that defences alone will not always prevent an organisation from suffering the negative consequences of a cyber attack. In order to build these aspects of cyber resilience, the organisation first needs to **identify** all of the assets that require protection (data, systems, etc.) and the things that threaten those assets. Technical, procedural, or physical controls can then be applied to those assets to ensure appropriate and proportionate security interventions are in place.

The University will adopt the Cybersecurity Framework (CSF) from the National Institute for Standards and Technology (NIST). This is an internationally-recognised framework, structured around the five key functions highlighted in Figure 2. An initial maturity baseline has been established, along with a target for how the University should aim to improve against each function. More information on the NIST CSF, including details of the categories that make up the five functions, can be found at **https://www.nist.gov/cyberframework**.

Figure 2: Cybersecurity framework

To identify more granular security controls, the University will use the related NIST Special Publication 800-53 (SP 800-53), Security and Privacy Controls for Information Systems and Organisations. This is a widely adopted catalogue of controls that can be tailored to different organisations. Appropriate control baselines will be defined for different types of system, balancing the need for security with the need for flexibility and accessibility. More information on SP 800-53 can be found at **https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final**.

How will we implement this?

The Information and Cyber Security Strategy is a significant undertaking that will affect all departments, colleges, institutes, staff, and students. To make the delivery manageable, it will be broken into four streams of activity (Figure 3).

Stream 1: Principles and framework
This stream formalises the University's principles, policies and standards for information and cyber security, many of which are already in place, and which will underpin the other streams.

Stream 2: Central systems
As centrally managed IT systems and services often host large volumes of confidential data and perform processes critical to multiple departments, this stream will focus on ensuring that such systems implement appropriate controls from SP 800-53, aligned to maturity targets against the CSF. This includes not only corporate systems, but central services such as the University's network, data storage, shared computing environments, and the Managed Desktop Service (MDS).

Stream 3: A university-wide security baseline
Although central systems may handle the largest volumes of confidential data, local systems and processes can also involve sizable volumes of data and be at risk of compromise. Furthermore, experience has shown that any system can be the entry point for a wider breach, even if that system itself is not particularly sensitive or critical. This stream will therefore work across departments, colleges, and institutes to understand risk, agree appropriate controls, and implement a consistent level of risk mitigation (Figure 4).

Stream 4: An information security management system (ISMS)
Information and cyber security is not a one-off initiative, but a systemic change that keeps the organisation protected on an ongoing basis. Threats are constantly evolving, while University processes and systems must also change to meet ongoing needs. An ISMS provides the framework to manage security risk, by embedding the necessary processes and procedures to ensure controls remain current and effective.

All the streams will make use of the NIST CSF and SP 800-53 in defining the appropriate policies, procedures, and technologies to protect the organisation and individuals.

"In both culture and technology, universities are one of the most open and outward facing sectors. This enables and eases collaboration between academics across borders, and is likely a key component of their success. Unfortunately, this also eases the task of an attacker."

National Cyber Security Centre, Sept 2019

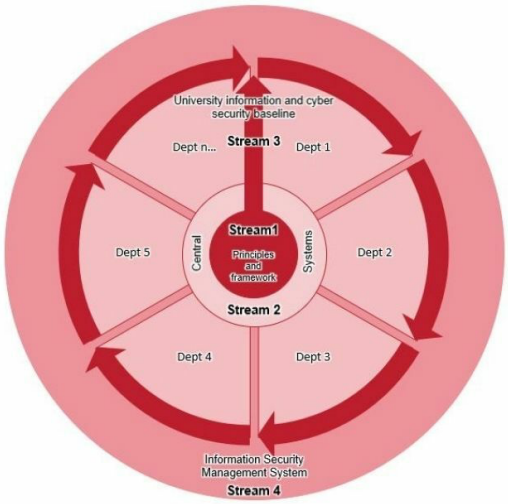


Figure 3: Four streams of activity

Figure 4: A University-wide security baseline

What does the strategy mean to me?

Improved information and cyber security benefit the University, its staff, students, alumni, and partner organisations. Some of the expected benefits are outlined in Figure 5. However, it can be achieved only with the support and engagement of everyone. Some of the things you will see as the strategy develops are detailed below.

- Policies to protect our security
- More information security awareness and training
- Identification and documentation of information and IT assets and who is responsible for them
- Risk assessments of information handling and IT systems
- Adoption of industry-standard controls for our IT systems
- System maintenance to keep environments protected
- Removal of legacy IT that cannot be effectively protected
- Auditing of information and IT controls
- Provision of improved data and functionality in central systems to reduce the need to store and handle sensitive data in multiple places
- Increased system monitoring to detect and respond to security threats and vulnerabilities, in some cases using automated responses
- Closer working between IGU, CIS, and other departments on information and cyber risk

"Protecting our people, data, and services is of the utmost importance, so we must build information and cyber security into the fabric of the University. This strategy is a living document that will help us to navigate competing demands in a consistent manner to best protect our institution."

Antony Long, Deputy Vice-Chancellor, Nov 2021

Figure 5: Benefits of improved information and cybersecurity

What happens next?

The University will establish a steering group to oversee the implementation of the strategy, with representation from across the organisation. The steering group will track progress in delivering the Strategy and ensure it is regularly reviewed to address the latest threats and risks to the organisation. A plan will be developed to implement the four streams of activity, starting in early 2022.

What can I do?

While the strategy will help us make a step change in our security there are things we can all do right now to protect ourselves and the University. Some examples are provided to the right, while more details and the latest advice can always be found on the CIS web pages, at the following link:
durham.ac.uk/cis/security/staysafeonline

- Use a strong password
- Think before clicking links and opening attachments
- Be suspicious of unexpected messages
- Keep your IT up to date
- Use up-to-date anti-malware
- Don't send sensitive data in email

Durham University

Inspiring the extraordinary

The Palatine Centre
Durham University
Stockton Road
Durham
DH1 3LE

OUT_9487089