Campaign implementation plan

This guidance is designed to support research organisations, including universities, to run campaigns which implement the advice and guidance outlined in Trusted Research for Academics and Guide for Senior Leaders.

Trusted Research aims to support UK universities and research institutions in making informed decisions about international collaboration and, in doing so, protecting their own researchers and academic values. The advice in Trusted Research has been produced in collaboration with universities and the research community in the UK.

This guide provides a practical framework to embed security behaviours and support an environment which sustains these behaviours within universities. The advice is based on a framework called Embedding Security Behaviours: using the 5Es.

WHO IS THIS GUIDANCE FOR?

This implementation guidance has been produced for the person (or teams) responsible for the security of research and personnel at your institution. It will help to implement and sustain the security behaviours appropriate for your institution with key stakeholders including:

- Academic staff and research groups (such as heads of department, principal investigators, post-doctoral researchers and students)
- Non-academic staff (such as legal departments, IT and cyber security staff, and departments responsible for buildings management, intellectual property (IP), human resources, international collaboration and trade)
- Spin-off companies which are associated or affiliated with your institution

Scoping your campaign

In order to implement a Trusted Research campaign based on the 5Es framework, it is crucial that your institution understands the security behaviours it requires from its employees. Each university is different and you will need to develop processes which work for your institution and staff (academic and non-academic) and complement your existing security arrangements.

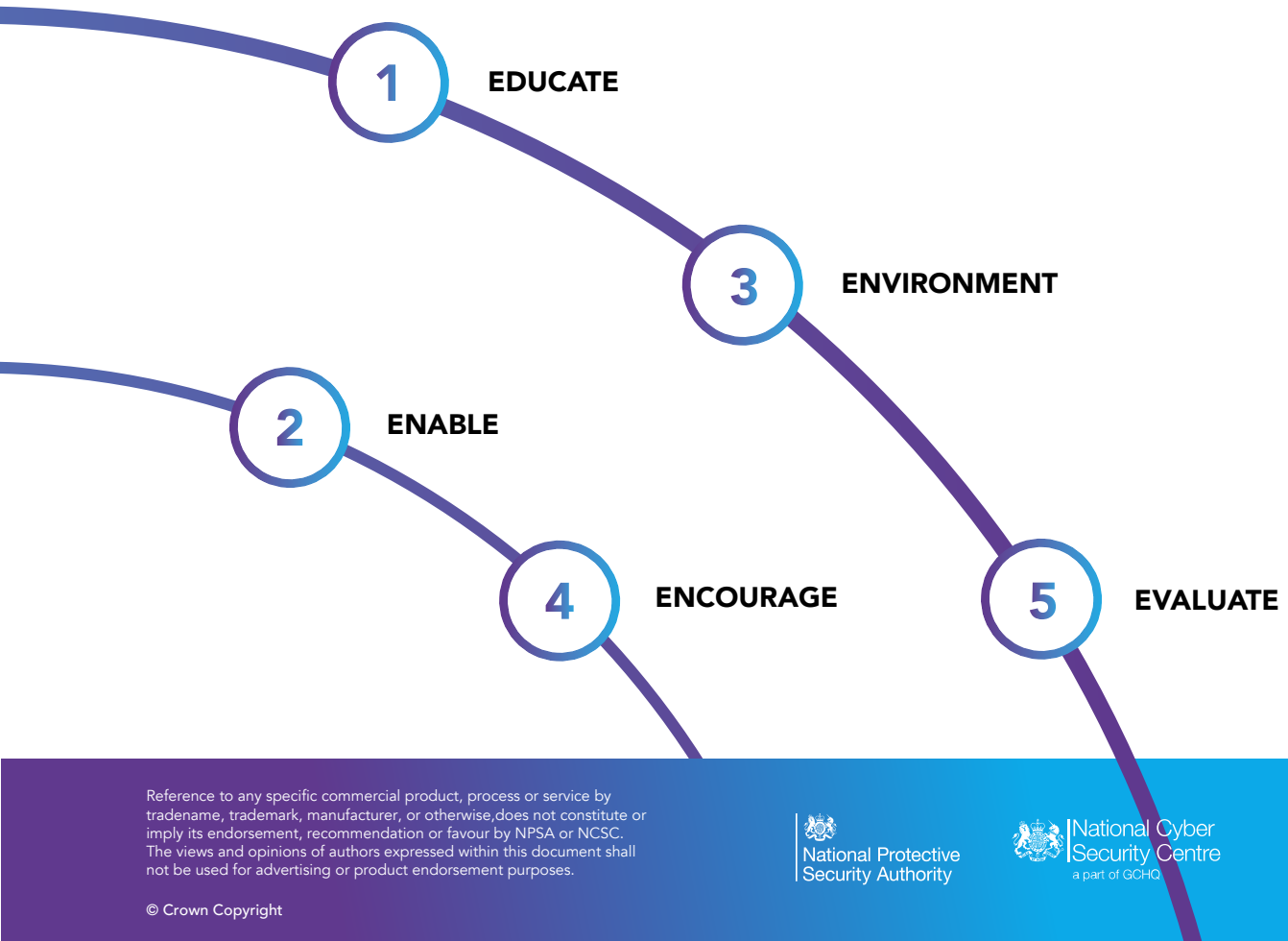
You may wish to consider the following questions:

- Which research and staff are most at risk?
- Do you understand the security threats that are currently facing your institution?
- What level of security risk are staff and research exposed to, particularly those involved in international collaboration?
- What is your university's risk appetite (and that of key collaboration and funding partners)?
- What level of protective and cyber security is appropriate at your institution?
- What interventions and changes will you need to introduce and embed to achieve this level of security? Will this augment any existing practices or replace them?

IMPLEMENTATION OF TRUSTED RESEARCH USING THE 5ES

Once your university has decided on the roles and behaviours it requires from its people to protect its research, staff and reputation, the 5Es framework can be used to embed and sustain security behaviours. This guidance is not directive as the structure and needs of each institution vary. Consider how you can adapt these principles for your institution. The following pages detail each stage of change management.

The 5Es



Educate

The base level of understanding of the threat to research from hostile states may vary between institutions as well as within each institution among different stakeholder groups. In this first phase of the framework:

- Educate staff on the security threat to them, their research and the institution
- Educate staff on the benefits to them of adopting the security behaviours and the consequences if they fail to do so
- Educate staff on why the threats matter to the institution

QUESTIONS TO ASK

Do you know who within your institution could be at risk from state actors hostile to UK interests?

Have you identified the relevant departmental areas or research groups that are most likely to be carrying out international collaboration?

These could be, but not limited to, researchers in STEM subjects, potential dual-use technologies (civil-military), emerging technologies and commercially sensitive research areas.

Do you and your research community know what research could be at risk?

This is most likely to be STEM subjects, potential dual-use technologies (civil-military), emerging technologies and commercially sensitive research areas where there is international collaboration or funding. You can ask heads of department or individual researchers to consider the questions below in relation to their ongoing and prospective research collaborations.

To assess which research could be at risk you might want to consider:

- Whether information about the application of these areas of research could cause any ethical or moral concerns for the institution, research group or individual academics
- Whether the research is likely to be subject to UK or other countries' export licence controls
- Whether the research contains sensitive data or personally identifiable information that is not available from open source or open source datasets that are combined in a unique way. This may include genetic or medical information, population datasets, details of individuals or commercial test data
- Whether the research is likely to have a future commercial or patentable outcome which you or your organisation would want to benefit from

Having identified stakeholders, such as specific researchers, groups or departments, what is the best way to reach them?

Could you, or relevant heads of department or group, facilitate a discussion of the key themes in Trusted Research with these groups?

How can this be best communicated? E.g. management briefings, intranet articles, departmental meetings.

Enable

Enable staff to adopt the security practices that are right and proportionate for them and the institution by providing easily accessible training and reference materials. Consider the following points:

- What security behaviours are expected of staff?
- Will this vary depending on their roles or involvement in sensitive research and international collaboration?
- What does each staff member or group need to do in order to demonstrate compliance with the institution's security policy?
- What is the best method of delivery for information and training to each target group? E.g. E-learning packages, team training, away days, a mentoring system
- Where should reference materials on security policies be accessed and stored?

GENERAL PRINCIPLES FOR TRAINING AND INFORMATION

Training should enable staff to:

- Understand the criteria and process for assessing whether research is sensitive or at risk
- Know what risk mitigations are appropriate or know where to seek advice
- Document the process of risk assessment and mitigation for sensitive research and international collaboration

Know where to report risk assessment and mitigation

- Know where to get advice on identifying, managing and documenting risk or security procedures

AREAS TO CONSIDER

Due diligence – what information is provided to schools, departments and/or researchers on the institution's requirements for due diligence for international partners?

Security of research and personal data – is training and information available for staff to support the security of research and data which is held on the university's network?

Your IT service department can assist you in developing security measures which meet your needs and are compatible with your IT systems. Further guidance is available via NCSC.gov.uk.

Legalities – do staff have appropriate information on legal compliance that includes export control, contracting, IP and GDPR (General Data Protection Regulations)?

Your agreements with international partners must comply with UK law, avoid harm to the UK's interests, and address potential threats to the integrity and reputation of your university.

Environment

Create an environment which makes it easy for staff to follow security processes; aim for this to become an accepted part of day-to-day working practice.

Consider the following:

- Does the current work environment make it easy for staff to follow security procedures? Are security processes simple to follow?
- Is security-related information easy to find?
- Do the necessary forms, processes and IT systems make it easy to comply with security practices?
- Do staff have easy access to the IT, materials and people they need to complete security?
- Does the social environment promote and normalise good security? Do managers and senior colleagues lead by example?
- Do peers support one another with security tasks and challenge a lack of security compliance?
- Is there a security champion in each team?

IDEAS TO SHAPE THE ENVIRONMENT

- Review existing security processes so they are easy to follow and fit for purpose
- Work with your IT department or provider to ensure IT systems meet security needs
- Include compliance with security in performance appraisals
- Provide security training on induction and regular top-up training to ensure that staff are up to date on threat, policy and processes
- Consider using tools, such as management briefing or blogs, in addition to posters, intranet pop-ups or other workplace reminders

Encourage

Encourage and sustain good security behaviour by providing feedback, as well as soft and hard incentives.

Consider the following:

- Provide feedback for staff, including acknowledgement and thank-you messages from the Head of Security, heads of department or other senior staff members which highlight good behaviours
- Provide feedback on security performance during career appraisals and team meetings
- Encourage feedback on security performance in meetings with external research partners and funders
- Publicise blogs and articles on positive and negative security case studies. These could be examples from your own or other institutions
- Provide soft and hard incentives to encourage good security
- Use incentives that will motivate your staff - academic and non-academic - and partner organisations most effectively. Thank staff for reporting a security concern or successfully managing a higher risk international collaboration
- Include compliance security requirements in contractual obligations and employment terms and conditions
- Include clauses in memoranda of understanding for international collaboration which include compliance with the security requirements set out by your institution

Evaluate

Your institution will want to evaluate the extent to which time, resources and costs involved have improved security and whether improvements or modifications of the process are required.

Evaluation will also provide evidence of your institution's recent track record on protecting research, which could provide reassurance and incentivise funding partners.

Identify your key performance indicators for measures of success against which your institution will evaluate progress.

These will vary for each institution but may include:

- Appointing a Head of Risk for International Collaboration or similar role responsible for managing the risk
- Creating and adopting a documented process to assess and manage risk for international research collaborations
- Adding compliance with security requirements to employment terms and conditions
- Including clauses in memoranda of understanding for international collaboration which require all parties to match your institution's security requirements

EVALUATION METRICS

Consider evaluation metrics prior to the implementation of a new security campaign as well as after to gain a better measure of the impact of your security improvements. Identify which metrics are currently available for institutions such as IT reports, memoranda of understanding, audits etc.

Augment by conducting staff surveys, focus groups or similar.

Endorsement

The effect of implementing a Trusted Research campaign through the 5Es framework will be enhanced if staff see that they are endorsed by credible sources. These can be both internal and external to the organisation, e.g. senior academics with experience of international collaboration, subject matter experts in areas such as hostile states, cyber security or risk managers.

When planning each phase of implementing security measures, think about who will be the voice of this phase of the campaign. Who can make the messages resonate with your stakeholders?

Different groups of staff may require endorsement from different people. Corporate staff may respond well to a briefing by the Head of Security or a security manager, whilst academics may relate best to endorsement by industry partners or academics in the same field.

The message must be visible and consistently endorsed from the top of the organisation. Leaders can endorse in a range of ways, including inclusion and dissemination of key messages on security, attendance at security events, briefings and blogs.

Consider the following:

- External speakers from industry or government funding bodies
- TED-style talks, articles and case studies from subject matter experts on the potential threat from hostile states
- Academics with experience of international collaboration talking about the benefits of protecting research
- Speakers and cast studies from other universities who are engaged in international research collaboration.
- Workshops and Q&As with security experts and risk management consultants
- Talks, blogs, briefings and articles from the Vice Chancellor, senior academics, heads of security and TTEOs on the importance of good research security

USEFUL LINKS AND REFERENCE MATERIALS

Embedding Security Behaviours Using the 5Es:
https://www.npsa.gov.uk/resources/embedding-security-behaviours-using-5es

Academic Technology Approval Scheme (ATAS):
https://www.gov.uk/guidance/academic-technology-approval-scheme

Responsibilities for General Data Protection Regulations (GDPR):
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

UK Export Control, the Department for International Trade Export Control Joint Unit (ECJU):
https://www.gov.uk/government/organisations/export-control-organisation

Intellectual Property Office (IPO) Lambert Toolkit:
https://www.gov.uk/government/publications/intellectual-property-for-business/ip-for-business-tools