Information Risk Management Policy

Updated on 31/01/2024

Review Date 01/02/2025

Responsible Person: Director – Shebul Ali

UK Graduate, 73 Greenfield Road, First Floor, London E1 1EJ
Tel: 020 3609 0260 |Email: info@ukgraduate.org.uk
www.UKGRADUATE.org.uk

UK Graduate Ltd Registered in England and Wales 09367578

This policy sets out the principles that the College uses to identify, assess and manage information risk

PURPOSE

Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

However, the implementation of controls to protect information must be based on an assessment of the risk posed to the College, and must balance the likelihood of negative business impact against the resources required to implement the controls, and any unintended negative implications of the controls.

This policy sets out the principles that the College uses to identify, assess and manage information risk, in order to support the achievement of its planned objectives, and aligns with the overall College risk management framework and approach.

This high-level Information Risk Management Policy sits alongside the Information Security Policy and Data Protection Policy to provide the high-level outline of and justification for the College's risk-based information security controls.

- **Information Security Policy**
- **Data Protection Policy**

OBJECTIVES

The College's information risk management objectives are that:

- Our information risks are identified, managed and treated according to an agreed risk tolerance
- Our physical, procedural and technical controls are agreed by the information asset owner
- Our physical, procedural and technical controls balance user experience and security
- Our physical, procedural and technical controls are cost-effective and proportionate.

SCOPE

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all information used at the College, in all formats.

This includes information processed by other organisations in their dealings with the College.

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all individuals who have access to College information and technologies, including external parties that provide information processing services to the College.

COMPLIANCE

Compliance with the controls in this policy will be monitored by the Information Security team and reported to the Director.

REVIEW

A review of this policy will be undertaken by the Information Security team annually or more frequently as required, and material changes will be approved by the Director and the College Executive Group.

POLICY STATEMENT

Information Risk Assessment is a formal and repeatable method for identifying the risks facing an information asset. It is used to determine their impact, and identify and apply controls that are appropriate and justified by the risks.

It is the College's policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals
- Integrity – the accuracy and completeness of information will be maintained
- Availability – information will be accessible to authorised users and processes when required

1. RISK ASSESSMENT

Risk assessments must be completed with access to and an understanding of:

- The College's business processes
- The impact to the College of risks to business assets
- The technical systems in place supporting the business
- The legislation to which the College is subject
- Up-to-date threat and vulnerability assessments

A risk assessment exercise must be completed at least:

- For every new information-processing system
- Following modification to systems or processes which could change the threats or vulnerabilities
- Following the introduction of a new information asset
- When there has been no review in the previous three years

A risk score is calculated from Likelihood x Impact Level, consistent with the College's high level Risk Management Policy.

2. THREATS

The College will consider all potential threats applicable to a particular system, whether natural or human, accidental or malicious.

The College will reference Annex C of the ISO 27005 standard to aid with threat identification.

Threat information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, and contacts across the sector and region.

It is the responsibility of the Director to maintain channels of communication with appropriate specialist organisations.

3. VULNERABILITIES

The College will consider all potential vulnerabilities applicable to a particular system, whether intrinsic or extrinsic.

The College will reference Annex D of the ISO 27005 standard to aid with vulnerability identification.

Vulnerability information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, technology providers and contacts across the sector and region.

It is the responsibility of the Director to maintain channels of communication with appropriate specialist organisations.

4. RISK REGISTER

The calculations listed in the risk assessment process will form the basis of a risk register.

All risks will be assigned an owner and a review date.

The risk register is held in the Information Security document store, with access controlled by the Information Security team.

5. RISK TREATMENT

The risk register will include a risk treatment decision. The action will fall into at least one of the following categories:

- Pending – where a potential risk has been identified but needs initial investigation. This should take place within 30 days. After 30 days the item is automatically changed to Treat if no one has evaluated the risk. This would then be passed to the Operations risk board who will take guardianship of it until the initial investigation is completed.
- Tolerate the risk – where the risk is already below the College's risk appetite and further treatment is not proportionate
- Treat the risk – where the risk is above the College's risk appetite but treatment is proportionate; or where the treatment is so simple and cost effective that it is proportionate to treat the risk even though it falls below the College's risk appetite
- Transfer the risk – where the risk cannot be brought below the College's risk appetite with proportionate treatment but a cost-effective option is available to transfer the risk to a third party
- Terminate the risk – where the risk cannot be brought below the College's risk appetite with proportionate effort/resource and no cost-effective transfer is available

The Information Security team in collaboration with the Information Asset Owner will review Medium and Low risks, and recommend suitable action.

The Director in collaboration with the Information Asset Owner will review High risks and recommend suitable action.

In the event that the decision is to Treat, then additional activities or controls will be implemented via a Risk Treatment Plan. These risks will be evaluated at least every 90 days. All risks in a Tolerate state will be evaluated at least annually.

6. ROLES AND RESPONSIBILITIES

The Director has accountability to the Executive Group and stakeholders for managing information risk.

The Director will direct the information risk appetite for the College and review the information risk register. The Director will be involved in assessing and reviewing High risks.

The Chief Information Security Officer is responsible to the Director for managing the risk assessment process and maintaining an up-to-date risk register. The Information Security team will conduct risk assessments and recommend action for Medium and Low risks, where these can be clearly defined in terms of the College's risk appetite.

The Director is responsible for assessing and reviewing High risks, and will have visibility of the risk register.

Information Asset Owners and Information Asset Managers must be responsible for agreeing and implementing appropriate treatments to risks under their control. They must also take an active role in identifying and reporting new risks.

7. RISK APPETITE AND TOLERANCE

The College has agreed a series of risk appetite statements.

While not exhaustive, these give a good overview of the College's desire to pursue or tolerate risk in pursuit of its business objectives.

The risk appetite statements give the Information Security team, and the Director, a framework within which to conduct risk assessments and make recommendations for appropriate treatments.