Glossary

Access control: Means to ensure that access to assets is authorised and restricted based on business and security requirements

Attack: Attempt to destroy, expose, alter, disable, steal or gain unauthorised access or to make unauthorised use of an asset

Authentication: Provision of assurance that a claimed characteristic of an entity is correct

Availability: Property of being accessible and usable upon demand by an authorised entity

Confidentiality: Property that information is not made available or disclosed to unauthorised individuals, entities or processes

Continual improvement: Recurring activity to enhance performance

Control: Measure that is modifying risk

Corrective action: Action to eliminate the cause of a nonconformity and to prevent recurrence

Event: Occurrence or change of a particular set of circumstances

Governance of information security: System by which an organisation’s information security activities are directed and controlled

Information security: Preservation of confidentiality, integrity and availability of information

Information security incident: Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
**Information security incident management:** Processes for detecting reporting, assessing, responding to, dealing with and learning from information security incidents

**Information system**: Applications, information technology assets or other information handling components

**Integrity**: Property of accuracy and completeness

**Level of risk**: Magnitude of a risk expressed in terms of the combination of consequences and their likelihood

**Likelihood**: Chance of something happening

**Monitoring**: Determining the status of a system, process or an activity

**Nonconformity**: Non-fulfilment of a requirement

**Policy**: Intentions and direction of an organisation as formally expressed by its top management

**Process**: Set of interrelated or interacting activities which transforms inputs into outputs

**Reliability**: Property of consistent intended behaviour and results

**Requirement**: Need or expectation that is stated, generally implied or obligatory

**Residual risk**: Risk remaining after risk treatment

**Review**: Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
**Risk**: Effect of uncertainty on objectives

**Risk acceptance**: Informed decision to take a particular risk

**Risk analysis**: Process to comprehend the nature of risk and to determine the level of risk

**Risk assessment**: Overall process of risk identification, risk analysis and risk evaluation

**Risk management**: Coordinated activities to direct and control an organisation with regard to risk

**Risk owner**: Person or entity with the accountability and authority to manage a risk

**Risk treatment**: Process to modify risk

**Sensitive Data**: Data that must be protected from unauthorised access to safeguard the privacy of an individual and/or the security of the College. Sensitive data includes personal data (see Data Protection policy for details), financial data and data related to intellectual property. (See Data Management policy for definitions of data types).

**Threat**: Potential cause of an unwanted incident, which may result in harm to a system or organisation

**Vulnerability**: Weakness of an asset or control that can be exploited by one or more threats