Information Security

&

Risk Management Policy

1. Introduction

1.1. Information that is collected, stored, analysed, communicated and reported upon is subject to possible misuse, loss, corruption and theft. To counter this our Organisation implements security measures and controls to protect information based on an assessment of the risk posed.

1.2. This assessment balances the likelihood of negative business impact versus the resources that are required to implement the controls (and indeed any unintended negative consequences of the controls).

2. Purpose

2.1. This Policy establishes the essential minimum standards for information security that must be met by Top Magic Limited.

2.2. Additionally, the purpose of this Policy is to also state the principles our Organisation will use to identify, assess and manage information risk, whilst aligning itself to the overall University of Reading risk management framework.

2.3. It permits entities to enhance these security measures based on their unique business requirements and the specific legal and federal guidelines applicable to them, but mandates that they at least meet the security benchmarks outlined herein.

3. Objectives

3.1. Serving as a foundational document, this Policy provides direction for all other security policies and related standards. It outlines the obligation to:

- Safeguard and uphold the confidentiality, integrity, and availability of information and its supporting infrastructure;
- Effectively manage the risks associated with security breaches or vulnerabilities;
- Ensure a secure and reliable information technology (IT) framework;
- Detect and act upon incidents involving the misuse, loss, or unauthorised access of information assets;

- Supervise systems for irregularities that may suggest security compromises; and
- Enhance and promote awareness of information security practices.

3.2. Inadequate security measures leading to compromised confidentiality, integrity, and availability of information assets can severely disrupt critical infrastructure operations, financial and business activities, and crucial governmental functions; endanger data; and result in legal and regulatory penalties.

3.3. This Policy ensures protective measures are adequately implemented to guard the confidentiality, integrity, and availability of information.

3.4. It also ensures that employees, affiliates and business associates are aware of their responsibilities, possess sufficient understanding of security policies, procedures, and practices, and are informed on how to safeguard information.

4. Scope

4.1. This information security Policy applies to all systems, both automated and manual, over which the entity has administrative control.

4.2. This includes systems that are managed or hosted by third-party services on the entity's behalf.

4.3. It covers all types of information, in any form or format, that are produced or utilised in the course of conducting business activities.

INFORMATION SECURITY:

5. Organisational Security Management

5.1. Effective information security necessitates the establishment of both an information risk management function and an information technology security function.

5.2. The configuration of the Organisation will determine whether these roles are combined and undertaken by either an individual or a group, or if separate individuals or groups are allocated for each function. It is advised that a senior executive or a team involving senior executives undertake these responsibilities.

5.3. Our Organisation has appointed a Chief Information Security Officer (CISO) to oversee risk management. This role entails assessing and providing advice on information security risks and ensuring that:

- The approach to risk for both information assets and specific information systems, including decisions on authorisation, is integrated and aligned with the broader strategic aims and foundational activities of the Organisation;
- The oversight of information assets and the management of risks related to information systems are uniform, mirror the Organisation's risk appetite, and are evaluated alongside other risk types to guarantee the success of the Organisation's mission and business operations; and
- The handling of the technical aspects of information security.

5.4. Decisions regarding information security risk must involve consultations with the functional areas mentioned above.

5.5. While the technical aspect of information security may be outsourced, the ultimate responsibility for the security of its information remains with the Organisation.

6. Functional Responsibilities

6.1. **Executive Management is tasked with:**

- Evaluating and accepting entity risks.
- Defining information security objectives and integrating them into processes.
- Ensuring the consistent application of security policies and standards.
- Demonstrating support for security through guidance and resource allocation.
- Raising security awareness via regular distribution of ISO materials.
- Managing information classification and protection based on best practices and legal requirements.
- Overseeing information asset management, including their use and disposal, according to classification.
- Assigning information owners while retaining overall responsibility for data protection.
- Engaging in security incident responses.
- Following breach notification protocols.
- Complying with legal and regulatory information security obligations.
- Informing the CISO or the Legal Compliance Department about legal and regulatory demands.
- Communicating Policy and standards requirements, including non-compliance consequences, to employees and third parties, ensuring third party contract compliance.

6.2. **IT Management is tasked with:**

- Guiding and integrating security measures into the data processing and network infrastructure to aid information owners.
- Allocating resources to uphold information security as per this Policy.

- Establishing and applying security processes, policies, and controls as specified by business needs and this Policy.
- Applying appropriate controls for information based on its classification.
- Training relevant technical personnel in secure practices.
- Encouraging the involvement of security and technical staff in safeguarding information assets and selecting efficient security measures.
- Executing business continuity and disaster recovery plans.

6.3. **The Chief Information Security Officer (CISO) is tasked with:**

- Offering internal security consultation.
- Formulating and implementing the security strategy and its effectiveness measures.
- Creating and upholding the Organisation's security Policy and standards.
- Verifying adherence to these policies and standards.
- Recommending secure system development practices.
- Managing incident response and providing expertise.
- Observing network irregularities.
- Keeping track of potential external threats like data breaches.
- Staying connected with security communities and authorities.
- Alerting to imminent threats and weaknesses.
- Supplying training materials and conducting awareness programs.

7. Duties Separation

7.1. Implement separation of duties to lower misuse risks. If infeasible, apply alternative controls like activity monitoring and management oversight.

7.2. Security control audit and approval must stay separate from their implementation.

8. IT Asset Management

8.1. Assign all IT hardware and software to a specific business unit or person.

8.2. Keep a detailed automated inventory of all hardware and software assets, noting key details like network address, machine name, and software version.

8.3. Use regular scanning to detect unauthorised hardware/software and alert relevant personnel.

9. Cyber Incident Management

9.1. Organisations must establish an incident response plan with consistent standards for effective security incident response.

9.2. Any detected or suspected security incidents or vulnerabilities must be promptly reported to the relevant supervisor / upper management and CISO as the designated security representative. Employees concerned about unaddressed cyber security issues can confidentially reach out to the Security Operations Centre.

9.3. The Security Operations Centre should be alerted to any cyber incidents with potential significant operational or security impacts, or those requiring digital forensics, to ensure appropriate response coordination and oversight.

10.Account Management & Access Control

10.1. Each account needs a designated individual or group for its management, potentially involving both the business unit and IT.

10.2. Access requires unique user-IDs, unless specified otherwise in the Account Management/Access Control Standard.

10.3. User-IDs must have an authentication method (e.g., password, biometric) for verifying identity.

10.4. Systems must lock after inactivity, displaying neutral information (e.g., screen saver), and require re-authentication.

10.5. Sessions must end automatically under defined conditions as per the standard.

10.6. Authentication tokens should be confidential and securely protected.

10.7. Tokens must be securely stored, if at all, with approved methods (e.g., password vault).

10.8. Information owners decide on access and privileges for their resources.

10.9. Access is based on job needs, adhering to the principle of least privilege.

10.10. Privileged account users must have a separate account for general business activities.

10.11. Systems should display a logon banner stating Policy compliance and monitoring.

10.12. Remote access requires prior approval, risk assessment, and documented controls.

10.13. Remote connections should occur through managed entry points as per ISO/security guidance.

10.14. Remote work needs management authorisation and secure data handling training.

11.Vulnerability Management

11.1. Systems must undergo vulnerability scans before production deployment and regularly after.

11.2. Regular penetration testing is mandatory for all systems.

11.3. Critical systems require periodic penetration testing.

11.4. Outsourced system vulnerability scans and penetration tests must be coordinated.

11.5. Contracts with third parties must include scan/test and mitigation obligations.

11.6. Scan/test results are to be promptly reviewed by the system owner and shared with the CISO as the designated security representative for risk assessment.

11.7. Discovered vulnerabilities must be promptly addressed through actions like patching, with a documented action and milestones plan for mitigation.

11.8. Only authorised individuals can conduct scans/tests, with prior notification to the CISO as the designated security representative. Unauthorised attempts are prohibited.

11.9. Authorised testers must adhere to a formal, tested process to avoid disruption.

INFORMATION RISK MANAEMENT:

- Systems supporting business must manage information risks and have annual risk assessments within a secure development lifecycle.
- New projects and major changes require security risk assessments.
- Entities choose their risk assessment method according to their needs and relevant regulations.
- Document assessment outcomes and related decisions.

12.Risk Assessment

12.1. Risks are assessed by considering the likelihood of occurrence and the impact a breach of data confidentiality, integrity and/or availability would have if it did occur.

12.2. Risk assessments shall be completed with appropriate/relevant understanding of and access to:

- The legislation to which the University is subject.
- The technical systems in place supporting the University.
- The impact to the University of risks to business assets.
- The University's business processes.

12.3. A risk assessment must be completed (at least) for the following:

- Information assets associated with any proposed new or updated systems.
- Information systems associated with information assets classified as restricted or highly restricted.
- Following the discovery of a new risk impacting a system.

13.Threats

13.1. The Organisation shall consider all high and critical threats that apply to a system whether deliberate or accidental.

13.2. Threat information shall be obtained from asset owners, users, incident reviewing, contacts across the sector and region, security consultancies, and local and national law enforcement agencies and security services.

14.Vulnerabilities

14.1. The Organisation shall consider all high and critical vulnerabilities that apply to a system.

14.2. Vulnerability information shall be obtained from internal sources (e.g. IT personnel, vulnerability scans etc.), technology providers, contacts across the sector and region, security consultancies, and local and national law enforcement agencies and security services.

15.Risk Register

15.1. The Impact x Likelihood risk score shall form the basis for the risk register. Risks shall be assigned owners alongside a review date and the risk treatment option/s taking place.

15.2. The risk register shall be restricted to those with a need to know.

16.Risk Treatment

16.1. The treatment option will fall into one or more of the following categories:

16.2. Risk avoidance (terminate) – There is no cost-effective action to reduce risk. Deciding not to proceed with activities that introduce unacceptable risk to the University.

16.3. Risk sharing (transfer) – Shifting part of the risk to other organisations. Common techniques include insurance and outsourcing.

16.4. Risk modification (treat) – Information risks are reduced to an acceptable level by introducing, removing or altering controls.

16.5. Risk retention (tolerate) – No additional action is required other than what is already in place.

16.6. Risk treatment options shall be selected based on the outcome of the risk assessment, and the expected cost/benefit of implementing the options.

16.7. The four options for risk treatment are not mutually exclusive. In some cases, the Organisation may benefit by using a combination of options such as reducing the likelihood of risks, reducing their consequences, and sharing or retaining any residual risks.

17.Residual Risk

17.1. Once the risk treatment plan has been defined, residual risk/s need to be determined. This involves an update of the risk assessment, taking into account the expected effects of the proposed risk treatment.

17.2. If the residual risk still does not fall within the Organisation's acceptable risk criteria, a further iteration of risk treatment may be necessary before proceeding to documented formal sign off via risk acceptance.

18.Risk Acceptance

18.1. In some cases, it may be necessary to accept risk despite it falling outside of normal acceptable risk parameters.

18.2. This may be necessary because (for example) the benefits accompanying the risks are very attractive, the cost of risk modification is too high, or because appropriate risk treatment cannot be applied within timeframes defined in Policy.

18.3. In such cases, the risk owner (e.g. information asset owner, system owner etc.) must complete a risk acceptance form that explicitly states the risk/s and includes a justification for the decision to override normal acceptable risk criteria.

18.4. Risk acceptance forms shall be reviewed and signed off by a member of the Organisation Directorate or an appropriate equivalent.

18.5. Deviation from any information security/cyber security Policy shall require risk acceptance.

19.Compliance

19.1. This Policy becomes active immediately upon publication. All members are required to adhere to the established enterprise policies and standards.

19.2. These policies and standards are subject to change at any time, and adherence to any revised policies and standards is also required.

19.3. Should adherence to this standard be impractical or technically unattainable, or if a departure from this Policy is required to facilitate a business function, entities must seek approval for an exception via the Chief Information Security Officer's exception procedure.

20.Contact Information

20.1. Submit all inquiries and requests for future enhancements to the Legal Compliance Department which is this Policy owner at: legal@top-magic.co.uk

Last Updated: 05 February 2026