

Information Security Policy

EAP Research Consultancy

EAP RESEARCH
CONSULTANCY

Purpose

Information that's collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation, as well as possible judgements being made against EAP Research Consultancy Limited.

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

Objectives

EAP Research Consultancy's security objectives are that:

- our information risks are identified, managed and treated according to an agreed risk tolerance
- our authorised users can securely access and share information in order to perform their roles
- our physical, procedural and technical controls balance user experience and security
- our contractual and legal obligations relating to information security are met
- our teaching, research and administrative activity considers information security
- individuals accessing our information are aware of their information security responsibilities
- incidents affecting our information assets are resolved and learnt from to improve our controls

Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used at EAP Research Consultancy, in all formats. This includes information processed by other organisations in their dealings with EAP Research Consultancy.

The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to EAP Research Consultancy information and technologies. This includes external parties that provide information processing services to EAP Research Consultancy.

Compliance monitoring

Compliance with the controls in this policy will be monitored by the Information Security Team and reported to the Information Governance Board.

Review

A review of this policy will be undertaken by either Director. This will be annually or as required, and will be approved by the board.

Policy Statement

It is EAP Research Consultancy'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

EAP Research Consultancy will implement an Information Security Management System based on certified standards as required. EAP Research Consultancy will be mindful of the approaches adopted by its stakeholders, including research partners.

EAP Research Consultancy will adopt a risk-based approach to the application of the following controls:

1. Information security policies

A set of lower-level controls, processes and procedures for information security will be defined, in support of the high-level Information Security Policy and its stated objectives. This suite of supporting documentation will be approved by the board, published and communicated to EAP Research Consultancy users and relevant external parties.

2. Organisation of information security

EAP Research Consultancy will define and implement suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security within EAP Research Consultancy.

EAP Research Consultancy will appoint:

- an Executive to chair the Information Governance Board and take accountability for information risk
- an Information Governance Board to influence, oversee and promote the effective management of EAP Research Consultancy information
- an Information Security specialist to manage the day-to-day information security function
- Information Asset Owners (IAOs) to assume local accountability for information management

- Information Asset Managers (IAMs) responsible for day-to-day information management

3. Human resources security

EAP Research Consultancy's security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training will be made available to all staff. Poor or inappropriate behaviour will be addressed.

Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

4. Asset management

All assets will be documented and accounted for. This includes:

- information
- software
- electronic information processing equipment
- service utilities
- people

Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

All information assets will be classified according to their legal requirements, business value, criticality and sensitivity. Classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

5. Access control

Access to all information will be controlled and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed, and will include consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. The separation of duties will be implemented, where practical.

6. Cryptography

EAP Research Consultancy will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.

7. Physical and environmental security

Information processing facilities are housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets. This includes those that are critical or sensitive, against forcible or hidden attacks.

8. Operations security

EAP Research Consultancy will ensure the correct and secure operations of information processing systems. This will include:

- documented operating procedures
- the use of formal change and capacity management
- controls against malware
- defined use of logging
- vulnerability management

9. Communications security

EAP Research Consultancy will maintain network security controls to ensure the protection of information within its networks. EAP Research Consultancy will also provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities. This is in line with the classification and handling requirements associated with that information.

10. System acquisition, development and maintenance

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to reduce any risks identified will be implemented where appropriate.

Systems development will be subject to change control and separation of test, development and operational environments.

11. Supplier relationships

EAP Research Consultancy's information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

12. Information security incident management

Guidance will be available on what constitutes an information security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated. The appropriate action to correct the breach will be taken, and any learning built into controls.

13. Information security aspects of business continuity management

EAP Research Consultancy will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters. This is to ensure their timely recovery in line with documented business needs. This will include appropriate backup routines and built-in resilience.

Business continuity plans must be maintained and tested in support of this policy. Business impact analysis will be undertaken, detailing the consequences of:

- disasters
- security failures
- loss of service
- lack of service availability

14. Compliance

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.

Currently this includes:

- data protection legislation
- the payment card industry standard (PCI-DSS)
- the government's [Prevent strategy](#)
- EAP Research Consultancy's contractual commitments

EAP Research Consultancy will use a combination of internal and external audits to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures. This will include:

- IT health checks
- gap analyses against documented standards
- internal checks on staff compliance
- returns from Information Asset Owners

Review of this document: annually by Dr Jonathan Hobson & Dr Daniel Ash (Directors)

Next review date: 10/07/2026