Security Information & Protection Policy

Policy Statement

E3 Recruitment will ensure the protection of all information assets within the custody of the Business.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

Purpose

Information is a major asset that E3 Recruitment has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Organisation maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at E3 Recruitment. The policy specifies the means of information handling and transfer within the Business.

Scope

This Information Protection Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the Organisation who have access to Information Systems or information used for E3 Recruitment purposes.

Definition

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Speech.

Risks

E3 Recruitment recognises that there are risks associated with users accessing and handling information in order to conduct official business.

This policy aims to mitigate the following risks:

- the non-reporting of information security incidents
- inadequate destruction of data
- the loss of direct control of user access to information systems and facilities

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

Policy Compliance

If any user is found to have breached this policy, they may be subject to E3 Recruitment disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from Tracie Norton.

Policy Governance

The following table identifies who within E3 Recruitment is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Director / Business Support Manager
Accountable	Director
Consulted	Managers
Informed	All Employees, All Temporary Staff, All Contractors

Security Information & Protection Policy

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by Tracie Norton.

References

The following E3 Recruitment policy documents are directly relevant to this policy, and are referenced within this document:

- Acceptable IT Usage Policy
- Software Policy
- Clear Desk & Screen Policy

Key Messages

- The Business must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF).
- Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until the Directors are satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
- PROTECTED and RESTRICTED information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing PROTECTED or RESTRICTED classified information to any external organisation is also prohibited.